Пароль защитит себя сам !

2013

Nyukers(C)

Варианты пароля для пользователя. Графический или символьный. Запомнить легко, узнать невозможно. Жестикуляция. Стереопароль. Пароли для планшетного и настольного ПК.

Оглавление

В наше время все имеют пароли. Пароли применяются для идентификации пользователя различных компьютерных системах и сетях. Паролями пользуются как обычные пользователи так и привилегированные: администраторы, аудиторы, модераторы. На защищенность пароля, т.е. его сложность, в каждой компании существует определенная политика. Подобная политика применяется и на различных сервисах в Интернет типа Facebook, Twitter, ВКонтакте.

Обычно такая политика требует выполнения следующих условий:
· пароль должен состоять как минимум из 8-ми знаков;
· пароль не должен иметь отношение к самому пользователю (быть похожим на фамилию, дату рождения, кличку собаки, прочее);
· пароль не должен быть словом, которое может быть найдено в словаре;
· пароль должен иметь комбинацию верхних и нижних регистров букв и специальных символов;
· неповторяемость 6-ти паролей в течение определенного периода времени.

Nyukers

Символьный пароль – варианты защиты.

С давних пор пользователи изобрели метод создания псевдослучайного пароля. Самый простой метод – необходимо взять слово и выполнить определенные действия на ним. Рассмотрим слово "Android" в качестве примера. Пользователи часто создают следующие пароли: "AnDrOiD" (чередующиеся верхние и нижние регистры), "diordnA" (изменяя направление), "roidAnd" (перетасовыванием слогов), "A2d4o6d8" (объединение цифр и букв). Однако, чем сложнее пароль тем сложнее его запомнить самому пользователю.

Пользователи которые имеют на своем компьютере клавиатуру с рус/лат шрифтом, используют пароли на родном языке с посимвольной заменой на латинские символы. Например пароль "Пролісок" будет выглядеть так "Ghjkbcjr". Этот способ несколько усиливает защищенность пароля, но опять же, бессилен против атаки с использованием расширенного словаря, который учитывает правила транслитерации. Например пары букв "кириллическая-латинская" на клавиатурах однотипны: "й/q", "я/z" и т.д. Следовательно не представляет большого труда угадать слово из словаря с заменой алфавита. Практика использования сложных паролей пользователями показывает, что последние, как правило, либо просто забывают такие пароли, либо стараются их сохранить "на память" в записных книжках, настольных календарях, мобильных телефонах. Разумеется защищенность паролей после таких записей сводится на нет.

Попыткой помочь пользователю была идея создавать пароль по первым буквам слов из какой-нибудь знакомой фразы. Например пароль из фразы "Еней був парубок моторний, і хлопець хоч куди козак" будет набор букв "Ебпміхчкк". Разумеется такое слово отсутствует в любом словаре. Но этому способу присущи и недостатки: теперь в уме надо держать всю фразу, а при смене неповторяющихся паролей в течение определенного времени надо обладать чуть ли не литературными способностями.

Следует заметить, что ни одна политика определяющая сложность пароля в организации не предлагает самому пользователю методику запоминания такого пароля не где нибудь, а только в уме. По крайней мере автор таких еще не встречал.

Поэтому уже давно назрела проблема совместимости, с одной стороны, легкости запоминания пароля, и с другой, высокого уровня защищенности пароля от перехвата и сложности его воспроизведения.

Графический пароль – такое возможно ?

Большинство компьютерных ОС много лет назад сделали переход на графический интерфейс. А принцип ввода паролей в этих система до сих пор остается символьним! Пользователи даже не предполагают, что пароль может быть не алфавитно-цифровым. Поскольку люди живут и работают в окружающем мире, где смысл человеческого зрения является доминирующим для большинства действий, наш мозг способен к обработке и хранению большого количества графической информации. В то время как мы, возможно, находим что очень трудно запомнить последовательность из десяти букв, в то же время мы можем легко запоминать лица людей, места, которые мы посетили, или обьекты, которые мы видели. Эти графические данные в электронном виде представляют миллионы байтов информации и обеспечивают большие возможности для уникальности выбора пароля. Поэтому, так называемые графические пароли являются более

Nyukers

"дружественными" для человека, в то же время увеличивая уровень безопасности [1].

Разгадывание графического пароля с помощью словаря неосуществимо в принципе, частично из-за большого пространства пароля, но большей частью, потому что нет никаких существующих доступных для поиска словарей для графической информации. Также трудно реализовать автоматизацию морфологического разгадывания. Тогда как мы можем признать лицо человека менее чем за секунду, компьютер затратит значительное количество времени на обработку миллионов байтов информации.

На основе этого компьютерщики в 2002 году изобрели вариацию защитной системы для аутентификации пользователя. Самое поразительное в ней то, что запомнить и воспроизвести пароль не сможет даже человек, стоящий рядом с монитором. При новых способах ввода пароля хакерам не поможет даже клавиатурный сниффер.

Пароль в новых системах — это не набор цифр или букв, а графическая картинка.

Например, пользователь должен щёлкнуть мышкой в четырёх точках (в пределах примерно десятка пикселей) на большой фотографии пейзажа. Пользователь компьютера может загрузить в программу любую понравившуюся ему фотографию. Главное, она должна обладать следующей особенностью: это должен быть достаточно разнообразный по виду пейзаж с множеством потенциально "интересных" мест. Когда пользователь создаёт пароль, он щёлкает на четырёх точках, которые ему лично легко запомнить: конкретное дерево, здание, складка местности (Рисунок 1.).

Рисунок 1.

Такой пароль, хранящийся в уме человека, и описать-то одним простым словом невозможно. Это зрительное впечатление, воспоминания и ассоциации. Но воспоминания надёжные. Тем более, что снимок может показывать знакомую только этому человеку местность. Подобрать же такой пароль крайне сложно. Сложно представить сколько может быть в кадре комбинаций из набора в четыре точки?

Также замечательно и то, что и самому пользователю будет не с руки записывать

Nyukers

такой пароль по привычке в записную книжку.

Существует способ введения пароля, который обладает ещё более удивительными свойствами. Так, даже если при наборе этого пароля за спиной пользователя будет стоять коллега и "случайно" запоминать все клики пользователя — он никогда не сможет зайти на машину вместо пользователя. Аналогично — если снимает камера системы наблюдения. Просмотрев видеозапись, никто не сможет восстановить ваш пароль. Дело в том, что при создании пароля пользователю предлагается выбрать и запомнить десять иконок примерно из сотни возможных. Иконки достаточно разнообразные. Представьте: при необходимости ввода пароля система выдаёт на экран сразу огромное панно из иконок, перемешанных случайным образом. Среди них обязательно будут три "ваши". Их следует мысленно соединить линиями (получится треугольник) и щёлкнуть мышкой в любой точке внутри этой фигуры (Рисунок 2.).

Рисунок 2.

Тут же иконки перестраиваются, перемешиваются. Одни при этом исчезают, другие — добавляются. И опять среди всего этого хаоса вы видите и какие-либо свои значки из той самой десятки (не обязательно те, что были на экране только что). Снова вы мысленно соединяете их в геометрическую фигуру и щёлкаете в любом месте, но опять-таки в её границах. И так происходит 10 раз. Лишь после 10 таких проходов машина однозначно идентифицирует иконки, которые вы мысленно держали в голове, выбирая место для щелчка. Но любой, кто будет за вами наблюдать, ни за что не угадает ваш пароль. При этом уровень секретности обеспечивается высочайший: "Если вы имеете достаточно многого изображений, и если вы должны пройти тест достаточно много раз, возможные комбинации иконок исчисляются миллиардами"[2].

Либо тот же вариант, но с цветными шариками, при этом каждый раз надо щелкнуть на шарике определенного цвета (Рисунок 3.).

Nyukers

Рисунок 3.

К сожалению два последниих метода являются более сложными к исполнению:
- не всякий пользователь сможет визуально на экране соединить линиями иконки (шарики), особенно если они будут расположены далеко друг от друга;
- если предлагать пользователю до 10 раз щелкать в новой картинке, то при наличии за спиной камеры видеонаблюдения это не увеличивает защищенность пароля, а, наоборот, ее уменьшает. Ибо в этом случае при просмотре видеозаписи можно провести анализ статистики расположения и наличия определенных иконок на экране. Если, конечно, на это есть время.

Стереопароль – нетрадиционная защита.

В связи с приведенным выше был предложен нетривиальный способ ввода графического пароля, который лишен отмеченных выше недостатков, хотя и требует от пользователя определенного внимания.

Было предложено использовать в качестве базовой картинки для графичекского пароля стереограмму. Как известно, стереограмма построена таким образом, что пользователь, чтобы увидеть ее без искажений должен находиться прямо перед экраном монитора. При этом глаза пользователя должны находиться на определенном фокусном расстоянии от поверхности экрана монитора [3]. Сама стереограмма, как базис для графического пароля создается предварительно с участием самого пользователя, т.е. в качестве трехмерных обьектов будут выбраны "знакомые" обьекты только этому пользователю. В качестве схемы ввода пароля можно использовать любую из вышеназванных, но с меньшим числом кликов на экране (Рисунок 4.).

Nyukers

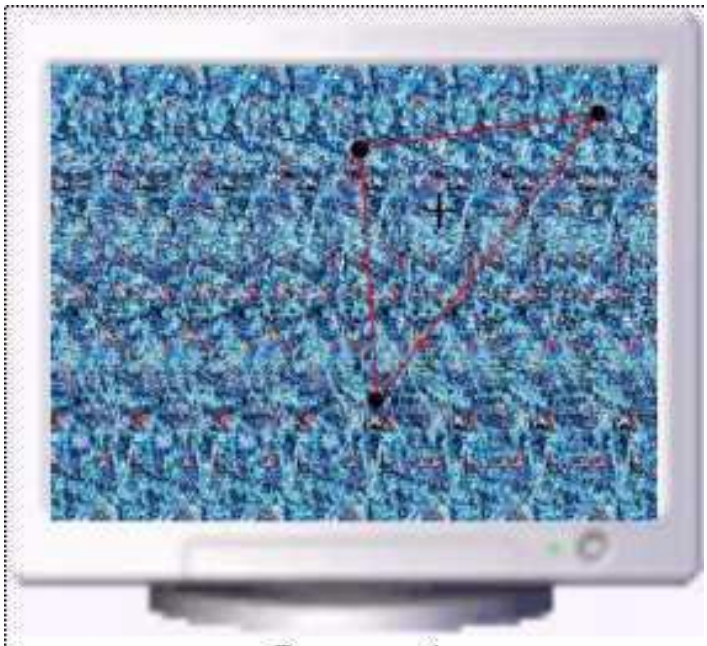


Рисунок 4.

Получается стереопароль. Основное преимущество стереопароля следующее – находясь под непрямым углом и на произвольном расстоянии от экрана монитора наблюдатель, будь то коллега пользователя или камера наблюдения, не сможет увидеть на экране ничего, кроме красивого узора.

Возможным недостатком можно назвать тот факт, что пользователь должен будет научиться фокусировать свой взгляд на стереокартинке. Но достигаемый при этом уровень защищенности личного пароля оправдывает все затраты.

Такой способ ввода графического пароля будет полезен для сотрудников с повышенной функциональной ответственностью, т.е. администраров, аудиторов, менеджеров, сотрудников служб безопасности и на тех рабочих местах, где наличие камеры видеонаблюдения предусмотрено технологией - кассиры, вахтеры. Возможно использование стереопароля для клиентов банкомата со встроенным touchpad-ом, где присутствие посторонних наблюдателей является естественным.

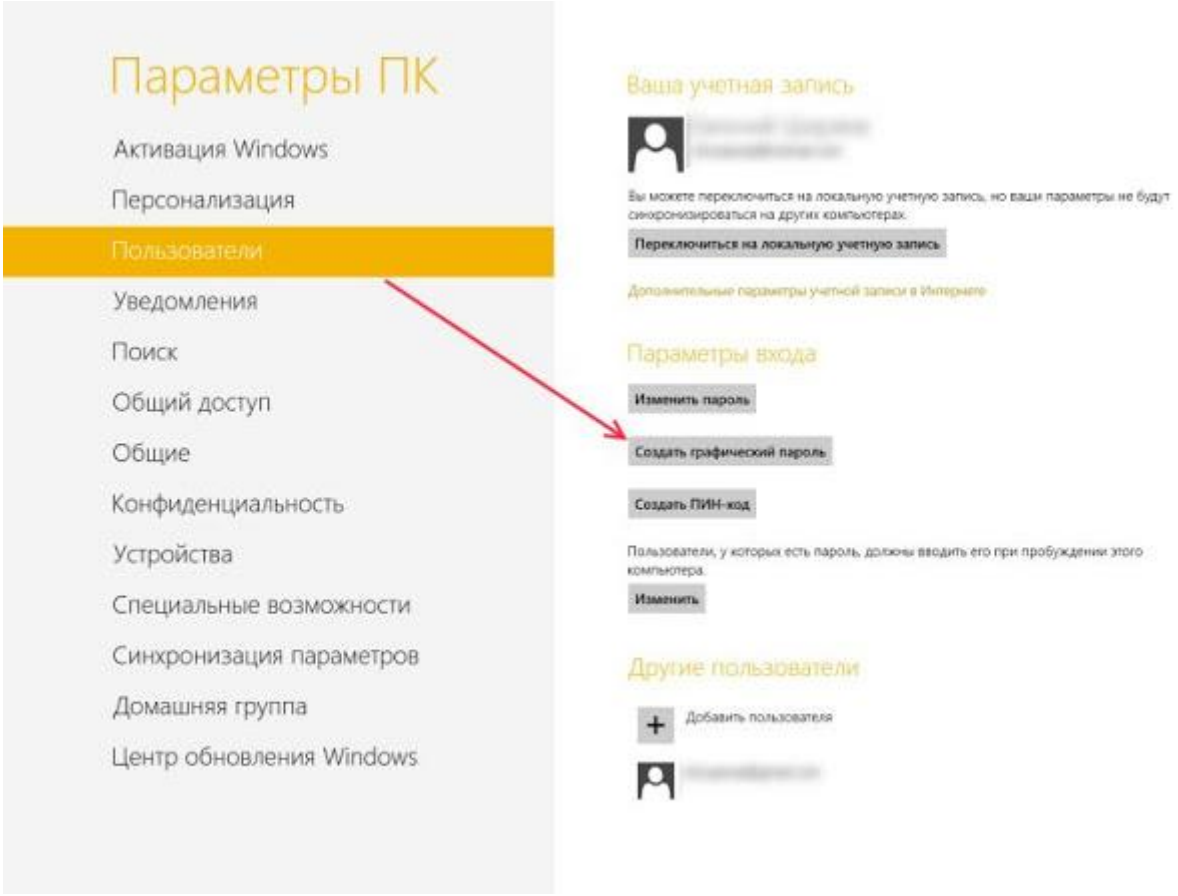
Windows 8 – графический пароль в массы.

Идея графического пароля оказалась не забыта и вот с выходом новой ОС Windows 8 в прошлом году мы наблюдаем его коммерческое применение. Интерфейс Windows 8 в первую очередь ориентирован на планшетные ПК, поэтому графические пароли в них предлагаются в качестве штатной опции. В первую очередь опция предназначена для владельцев сенсорных экранов и для удобства ввода ими пароля жестами для доступа к устройству, ведь сделать это можно гораздо быстрее, чем вводить длинные символьные пароли. Тем не менее владельцы стационарных ПК и ноутбуков оснащенными мышью также могут воспользоваться этой интересной функцией.

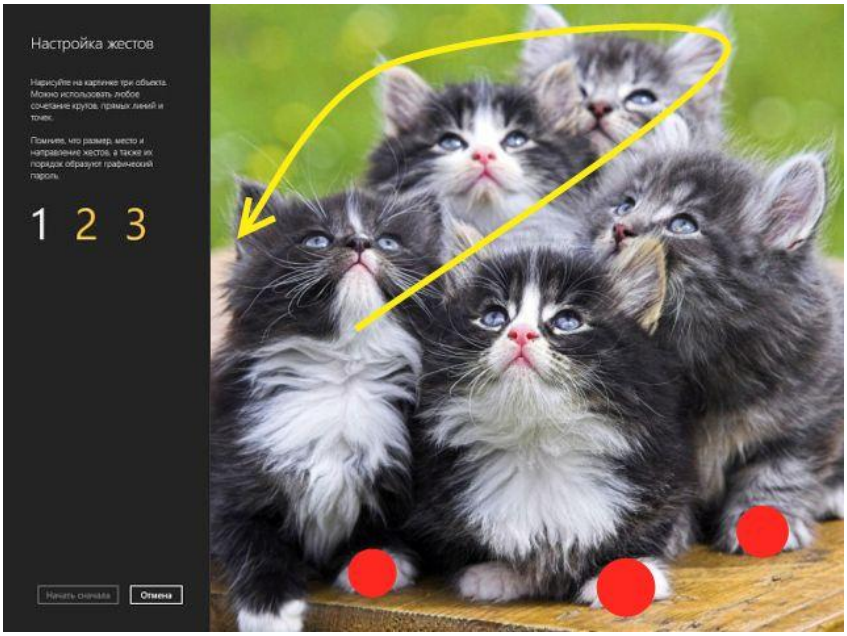
Прежде чем это использовать надо найти подходящую картинку, что нибудь яркое. Следующее, что нужно сделать это выбрать «Пользователи», а затем «Создать

Nyukers

графический пароль». При это у вашей учетной записи должен быть создан обычный символьный пароль, если его нет – создайте, после этого появится ссылка на создание графического.



Далее вам необходимо создать три жеста – действия на выбранном изображении, сделать это нужно будет два раза как и с обычным паролем, один раз и второй для подтверждения. Очень важно запомнить направление жестов, будь это линия или круговое движение, а также их расположение и места кликов.



Nyukers

После того как вы выбрали изображение для пароля, на нем формируется сетка. Самая длинная сторона изображения разбивается на 100 сегментов, затем разбивается короткая сторона и создается сетка, по которой рисуются жесты. Отдельные точки ваших жестов определяются их координатами (x, y) на сетке. Для линии запоминаются начальные и конечные координаты и их порядок, используемый для определения направления рисования линии. Для окружности запоминаются координаты точки центра, радиус и направление. Для касания запоминаются координаты точки касания. При попытке выполнения регистрации с помощью графического пароля введенные жесты сравниваются с набором жестов, введенных при настройке графического пароля. Рассматривается разница между каждым жестом и принимается решение об успешности проверки подлинности на основе найденного количества ошибок. Если тип жеста неправильный (должен быть круг, а вместо него линия), проверка подлинности не будет пройдена. Если типы жестов, порядок ввода и направления совпадают, то рассматривается, насколько эти жесты отличаются от введенных ранее, и принимается решение о прохождении проверки подлинности.

Следует помнить что графический пароль добавлен в качестве способа регистрации в системе как дополнение к текстовому паролю, а не вместо него ! Поэтому если вы все-таки забудете графическую комбинацию, то всегда будете иметь резервную возможность войти, введя свой символьный пароль.

Вместе с тем стоит учесть, что аутентификация в Windows 8 возможна и с помощью учетной записи Live ID [4], биометрической аутентификации, а также кода PIN. В более старых версиях операционной системы пароль на домашних компьютере хранился в файле SAM. Соответственно, для компрометации этого пароля злоумышленнику нужен был физический доступ к системе и привилегии SYSTEM. Что же получается сегодня? С выходом Windows 8 потенциальному злоумышленнику будет куда легче скомпрометировать систему, потому что в системе аутентификации появились новые слабые звенья. Естественно, хакеру потребуется просто найти наиболее уязвимое из них. Например, возьмем регистрацию в системе с помощью Live ID. Для конечного пользователя это несомненное удобство: забыл пароль — зашел на сайт Live ID с другого компьютера, воспользовался услугой смены пароля — и можно регистрироваться на своем компьютере с новым паролем. Но, несомненно, это и повышает шансы злоумышленников. Опять-таки, пользователь будет работать за другим компьютером, пароль к Live ID может храниться вместе с остальными паролями в браузере и т. д. И что самое интересное, и пароль Live ID, и PIN, и графический пароль, и биометрический — все они используются для дополнительного хранения и шифрования обычного пароля для реги- страции в системе. Поясню, почему эти звенья связаны с обычным паролем. Если пользователь выбрал аутентификацию по графическому паролю, то, в сущности, сам графический пароль применяется в качестве ключа для хранения и шифрования обычного пароля. Таким образом, получается, что, кроме SAM, обычный пароль будет храниться еще в одном месте. Если пользователь выбрал регистрацию с Live ID, то обычный пароль (текстовый, но зашифрованный с помощью Live ID) будет храниться в третьем месте и т. д. Таким образом, узнав пароль Live ID, несложно восстановить и оригинальный текстовый пароль.

Очевидно что на планшетах удобно рисовать линии и круги пальцем. Но такие же действия куда трудней будет повторить мышкой. У меня будут десятки вариантов соединения прямой линией двух точек интереса на фотографии. Просто потому, что я не смогу провести прямую линию мышкой. Поэтому

Nyukers

линия будет кривой. И эта кривая каждый раз будет разной. Точно так же с кругами и другими фигурами. Это дано далеко не каждому, слева пример того что получилось мышкой у меня. Для настольного ПК в качестве пароля хватило бы указать несколько точек интереса, кликнув по ним мышкой в нужном порядке. Примеры в начале статьи.

Таким образом сделать процесс аутентификации в Windows 8 более простым для пользователя удалось. А вот сделать защиту аутентификации более устойчивой пока нет. Возможно такой шаг Microsoft продиктован желанием потеснить популярную операционную систему для планшетов от Google-a Android, где такая защита сейчас названа графическим ключом. Хотя в Android графический ключ (матрица 3x3 без рисунка) предлагает гораздо меншую защиту чем графический пароль в Windows 8. Может потому что Android бесплатна?

Жестикуляция в цифрах.

Этот раздел доказывает преимущества графических паролей в цифрах и полностью цитирует Steven-a Sinofsky [5].

«При рассмотрении вопроса о количестве жестов, необходимых для задания графического пароля, мы учитывали надежность, запоминаемость и скорость ввода пароля. Требовалось найти баланс между этими, зачастую конкурирующими, свойствами и добиться оптимального взаимодействия с пользователем, которое будет также обеспечивать безопасность. Чтобы определить необходимое количество жестов, соответствующее нашим целям в плане безопасности пароля, мы сравнили графический пароль с другими способами проверки подлинности, а именно с ПИН-кодом и простым текстовым паролем.

Анализ количества уникальных комбинаций ПИН-кода довольно прост. В 4-разрядном ПИН-коде (4 разряда с 10 независимыми возможными значениями в каждом разряде) может быть 10^4 = 10 000 уникальных комбинаций.

Анализ текстовых паролей может быть упрощен, если предположить, что пароли — это последовательность знаков, состоящая из строчных букв (26), прописных букв (26), цифр (10) и символов (10). В простейшем случае, когда пароль состоит только из ***n*** строчных букв, возможны $\mathbf{26}^{\boldsymbol{n}}$ перестановок. Если пароль может иметь длину от 1 до ***n*** букв, количество перестановок будет *следующим*:

$$\sum_{i=1}^{n} 26^n$$

Например, 8-буквенный пароль имеет 208 миллиардов возможных комбинаций, что большинству пользователей покажется весьма безопасным количеством.

К сожалению, большинство пользователей выбирают пароли отнюдь не случайным образом. Для своих собственных устройств люди используют обычные слова и фразы, имена членов семьи и т. д.

Для подобного случая предположим, что пользовательский пароль состоит из двух строчных букв, одной прописной буквы, одной цифры или символа; прописная буква и цифра или символ могут находиться в любом месте в пароле. Количество уникальных паролей будет равно следующему значению:

Nyukers

$$26^{n-1} \cdot 20 \cdot \frac{n!}{(n-2)!}$$

В следующей таблице показано, как размер пространства решений меняется в зависимости от размера пароля и используемого набора знаков.

Длина пароля	**Уникальные пароли**
1	нет
2	нет
3	81 120
4	4 218 240
5	182 790 400
6	7 128 825 600
7	259 489 251 840
8	8 995 627 397 120

При рассмотрении графического пароля мы можем провести подобный анализ для каждого типа жеста. В приведенных ниже таблицах учитывается количество уникальных позиций жестов и степень мягкости нашего алгоритма распознавания.

Для простейшего жеста (касания) количество уникальных наборов жестов вычисляется как функция от количества касаний:

Число касаний	**Уникальные жесты**
1	270
2	23 535
3	2 743 206
4	178 832 265
5	15 344 276 658
6	1 380 314 975 183
7	130 146 054 200 734
8	13 168 374 201 327 200

Круговой жест сложнее касания, но проще линии. В попытке оценить относительную надежность кругового жеста предположим, что злоумышленник знает о том, что радиус гарантированно будет между 6 и 25 (что упрощает подбор кругового жеста), предположим далее, что координаты X и Y расположены между 5 и 95. Это дает злоумышленнику следующее пространство решений для исследования:

$$(95 - 5 + 1)^2 \cdot (25 - 6 + 1) \cdot 2 = 331{,}240$$

Для круга количество уникальных наборов жестов задается как функция от количества кругов:

Число	**Уникальные жесты**

Nyukers

кругов	
1	335
2	34 001
3	4 509 567
4	381 311 037
5	44 084 945 533
6	5 968 261 724 338
7	907 853 751 472 886

Линия — наиболее сложный из всех трех жестов. Линия определяется двумя точками на нормализованной сетке размером 100 x 100 и порядком задания этих точек, что номинально дает 100 миллионов возможных линий; однако длина линии должна быть не меньше 5, так что количество уникальных линий будет равно 99 336 960. В отличие от попыток подобрать круговые жесты, где злоумышленники могут делать упрощающие предположения, существенно сужающие пространство решений, для линий нет подобных очевидных методов редукции. Линии запросто могут быть короткими отрезками или идти от края до края экрана. Количество совпадений для линий будет следующим:

Число линий	Уникальные жесты
1	1 949
2	846 183
3	412 096 718
4	156 687 051 477
5	70 441 983 603 740

Разобравшись с надежностью отдельных жестов, мы можем объединить эти данные для оценки наборов, содержащих несколько жестов. Для этого просуммируем количество уникальных жестов каждого из трех типов жестов для определенной длины жеста *n* и возведем сумму в *n*-ю степень. Результаты приведены в следующей таблице, в которой графический пароль сравнивается с ПИН-кодом и текстовым паролем.

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	2 554
2	100	676	нет	1 581 773
3	1 000	17 576	81 120	1 155 509 083
4	10 000	456 976	4 218 240	612 157 353 732
5	100 000	11 881 376	182 790 400	398 046 621 309 172
6	1 000 000	308 915 776	7 128 825 600	
7	10 000 000	8 031 810 176	259 489 251 840	
8	100 000 000	208 827 064 576	8 995 627 397 120	

Nyukers

Как можно заметить, использование трех жестов обеспечивает значительное количество уникальных комбинаций жестов и такую же надежность, как у пароля из 5-6 случайно выбранных знаков. Кроме того, три жеста позволяют получить графический пароль, который легко запоминается и быстро вводится.»

Банкомат с белым экраном – это нормально.

Совсем недавно была опубликована идея от Dimovi[6] по которой он в частном порядке переделал свой старый монитор в "приватный", т.е. такой на котором без специальных очков вообще ничего увидеть невозможно! Это связано с особенностями поляризационной пленки, которая используется при изготовлении LCD–мониторов. Я полагаю что идею по изготовлению такого монитора можно направить в более полезное русло. А именно - задействовать такой монитор для банкомата. Преимущества банкомата с таким монитором были бы очевидны: клиент подходит к банкомату, берет прилагающиеся очки и производит на банкомате необходимые операции. Все защищено, экран для всех любопытных абсолютно белый. Безопасность на высоте.

Конечно, завтра на улицах вы не увидите таких банкоматов, но через пять лет все может быть. Ведь для внедрения идеи графического пароля понадобилось 10 лет !

Литература.

1. G.Blonder, "Graphical Passwords", US patent 5559961, 1996.

2. Graphical passwords, Leonardo Sobrano, Jean-Camille Birget, The Rutgers Scholar, An Electronic bulletin of Undergraduate Research, vol 4., 2002.

3. Е.А. Завальнюк, «Нарисуй мне пароль» – PC World, 6/2006, с.110-113.

4. В.Безмалый, Д.Нефедов, “Применение графического пароля в Windows 8” – Windows IT Pro/RE, 10/2012, с.45-47.

5. Steven Sinofsky, «Выполнение входа с помощью графического пароля», http://blogs.msdn.com/b/b8_ru/archive/2011/12/22/signing-picture-password.aspx

6. Dimovi, «Privacy monitor hacked from an old LCD Monitor», http://www.instructables.com/id/Privacy-monitor-made-from-an-old-LCD-Monitor/

Как связаться с автором.

Вопросы, комментарии или предложения можно написать автору по следующему адресу электронной почты: mailto:nyukers@gmail.com

Канал **«Nyukers WebTV – только позитивное видео»**
http://youtube.com/nyukers
Блог **«Мультимедиа блог в облаках»**
http://nyukers.blogspot.com
Сайт **«Nyukers Media Age – свобода творчества !»**
http://nyukers.ucoz.net

Автор будет весьма признателен за конструктивные замечания и интересные отзывы.