УДК 004
ВАК 05.13.17
РИНЦ 28.00.00, 50.00.00

С.Н. Давыдов, М.Я. Клепцов, Л.В. Любимова

Процесс аутентификации с применением графических паролей

В статье авторы рассматривают применение графических паролей при аутентификации. Главным преимуществом такой аутентификации является удобство для пользователей. Однако при многократном наблюдении сеанса входа в систему злоумышленник может понять пароль. Чтобы избежать этого недостатка, авторы рекомендуют использовать динамические графические пароли. На примерах трех динамических графических аутентификаций в статье показано, как, оставаясь удобным для пользователя, графический пароль может быть устойчивым.

Ключевые слова: *авторизация, аутентификация, графический пароль, динамические графические пароли, злоумышленник, информационная система, пользователь.*

THE AUTHENTICATION PROCESS USING GRAPHICAL PASSWORDS

In this article the authors review the using of graphical passwords for authentication. The main advantage of this authentication is the users friendly approach. However, with multiple browsing of the logon session, the attacker can see and understand the password. To avoid this drawback, the authors recommend to use dynamic graphical passwords. On three examples of dynamic graphical authentication article demonstrates how with user-friendly, graphical password can be stable.

Keywords: *attacker, authentication, authorization, dynamic graphical passwords, graphical password, information system, user.*

Введение

Аутентификация является одним из первых барьеров, появившихся в информационных системах и реализующих множественный доступ к информационным ресурсам. Более 20 лет именно она стоит на первом рубеже контроля. Очевидно, что среди основных достоинств этой методики защиты – её привычность и простота.

Однако 80% инцидентов в сфере информационной безопасности случаются вследствие использования слабых паролей – к такому выводу пришла компания Trustwave по результатам собственного исследования (2011 год), охватившего ряд компаний в 18 регионах мира. Аналитики посвятили исследование уязвимости элементов в системах информационной безопасности, в процессе которого изучили более 300 инцидентов. Главное заключение, сделанное в итоге: слабые пароли пользователей в информационных системах – наиболее уязвимое место, используемое злоумышленниками, как в крупных, так и в небольших компаниях.

Слабый пароль – это плохо, но обратная сторона применения сложных паролей – трудность удержания в памяти человека. Как следствие – небрежность их хранения в виде рабочих записей, а значит, злоумышленнику не составит особого труда получить эти сведения. Для создания пароля обычно ставится множество ограничений: определенное количество и состав символов, невозможность (нежелательность) использования дат, слов, которые можно найти в словаре.

Решения проблемы видится в многофакторной аутентификации. Но в связи с её дороговизной и необходимостью использования дополнительных аппаратных средств компании не всегда стремятся использовать данный вид защиты.

Однако хоть человеку и тяжело запомнить сложный буквенно-цифровой пароль, зрительная память на изображения работает куда лучше. Поэтому возможно применение графических паролей, самостоятельно или вместо обычных паролей в двухфакторной аутентификации.

Графический пароль – метод аутентификации, когда для доступа в систему пользователю необходимо выполнить некоторые операции над изображениями, например выбрать один или несколько заранее определенных объектов. Графические данные обеспечивают большие возможности для уникальности выбора пароля. Таким образом, графические схемы паролей дают возможность сделать пароли более понятными человеку при одновременном повышении уровня безопасности.

Применение графических паролей в настоящее время распростра-

Сергей Николаевич Давыдов,
математик 1 категории
Тел.: (499) 262-86-55
Эл. почта: davidovsn@gvc.rzd
ГВЦ ОАО «РЖД»
http://rzd.ru/

Sergei N. Davydov
Mathematician 1 category
Tel.: (499) 262-86-55
E-mail: davidovsn@gvc.rzd
MCC JSC «Russian Railways»
http://www.rzd.ru/

нено большей частью в мобильных и портативных устройствах с сенсорными экранами и ограничивается статическими паролями. Примеры такой аутентификации мы можем видеть на устройствах с операционными системами Android, IOS и Windows (рис. 1).

Самый большой недостаток «обычных» статических графических паролей – проблема подглядывания через плечо. Хотя графические пароли трудно угадать, человек, который наблюдал несколько сеансов входа в систему, может в зависимости от схемы, в конце концов, понять пароль. Однако этого недостатка можно избежать, используя динамические графические пароли.

Суть метода динамических графических паролей заключается в том, что пользователю известен определенный алгоритм и, зная его и свои парольные изображения, он может определить пароль для текущей сессии. Плюсы очевидны: запомнить алгоритм и сами изображения пользователю легче, чем запомнить сложный буквенно-цифровой пароль, который к тому же приходится периодически менять.

При этом даже если процесс аутентификации смогут наблюдать посторонние люди, это не понизит безопасность процесса. Каждый раз пользователь будет выбирать различные изображения (вводить различные данные), что не позволит злоумышленнику увидеть сами парольные изображения.

Плюсом также является то, что вариантов аутентификации можно предложить множество. Их количество ограниченно лишь фантазией разработчика и сложностью реализации. Для лучшего понимания рассмотрим примеры динамической графической аутентификации.

Пример 1. «Пересекающиеся прямые»

Для данного способа будут использоваться две картинки. На экране для ввода пароля в произвольном порядке разбросаны изображения. Правильный пароль – те из них, что находятся на пересечении прямых, выходящих из парольных изображений. Если правильные изображения находятся на одной прямой, то пароль – сами эти изображения. Алгоритм данного типа аутентификации представлен на рис. 2, пример – на рис. 3.

Для уменьшения вероятности случайного подбора пароля его ввод необходимо произвести 3 раза. Авторизация считается успешной, если пользователь не допустил ни одной ошибки.

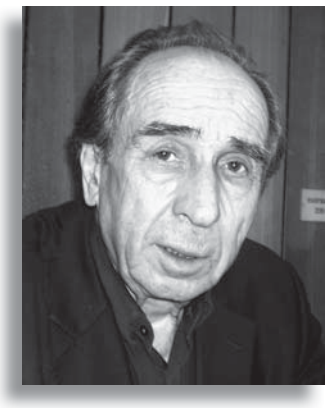
Вероятность пройти авторизацию, угадав пароль:

$$P_g = \left(\frac{1}{n} * \frac{1}{n-1}\right)^k,$$

где n – количество парольных изображений, k – количество раз, которое необходимо ввести пароль. Увеличивая n и k, можно повысить безопасность системы.

a) *Android* **b)** *Windows* **c)** *IOS (iPhone)*

Рис. 1. *Графические пароли в разных ОС*



Михаил Яковлевич Клепцов,
д.т.н., профессор
Тел.: (916) 016-37-80
Эл. почта: mkleptsov@mail.ru
МГУПС (МИИТ)
http://miit.ru/

Michael Ya. Kleptsov,
Doctor of Science, Professor
Tel.: (916)016-37-80
E-mail: mkleptsov@mail.ru
Moscow State University of Railway Engineering (MIIT)
http://www.miit.ru/

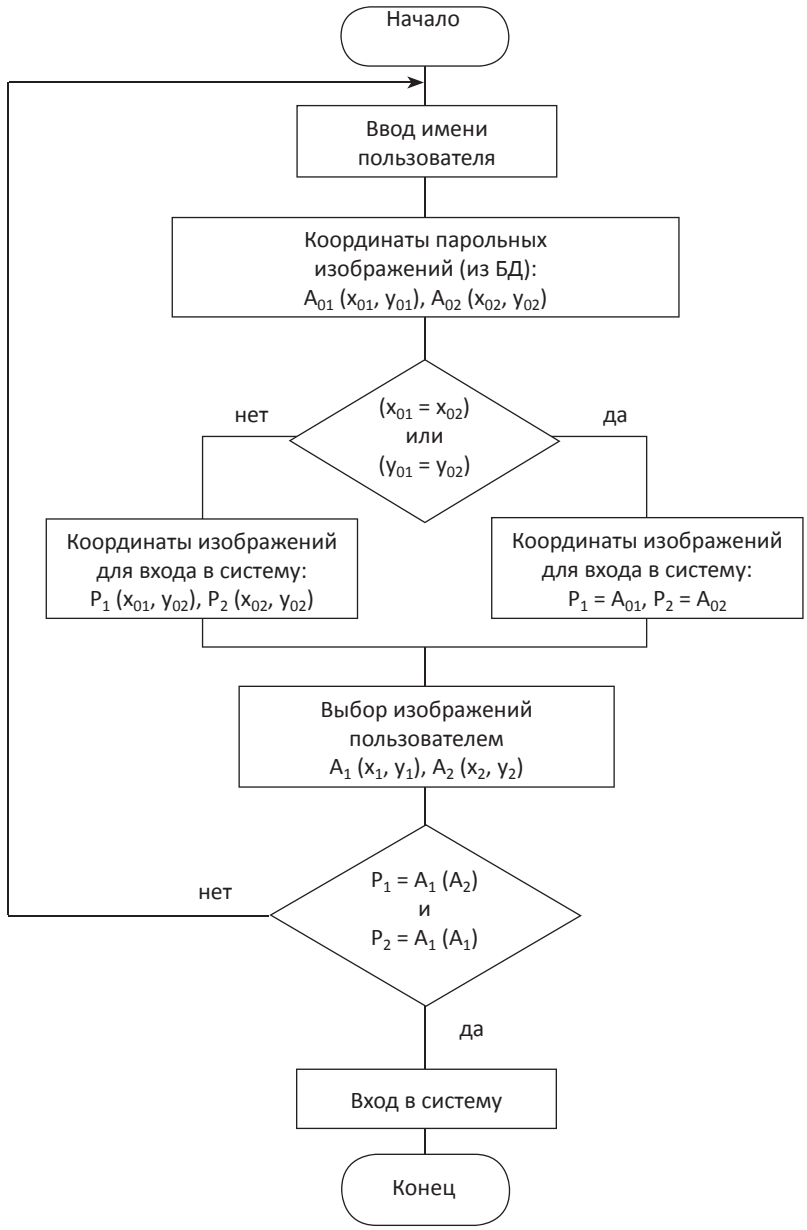


Рис. 2. *Схема аутентификации методом «пересекающихся прямых»*

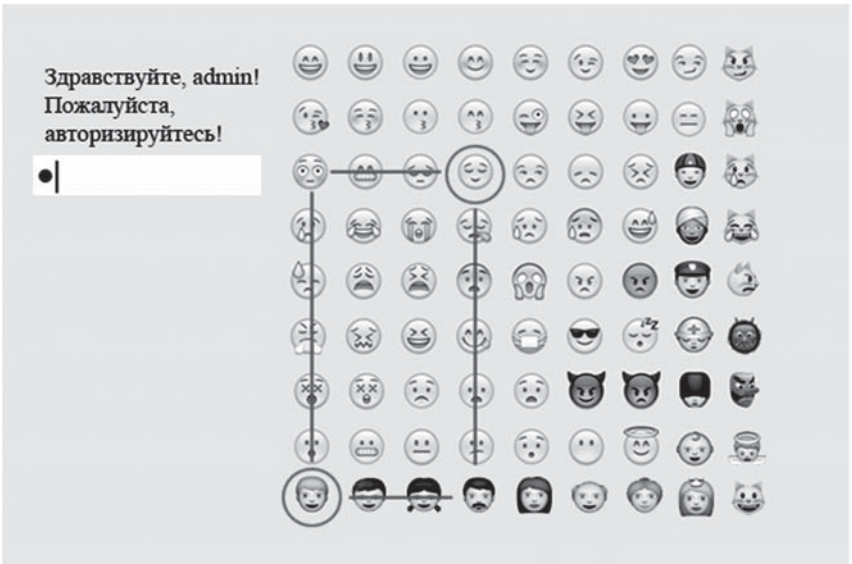


Рис. 3. *Метод «пересекающиеся прямые»*

В данном случае $n = 81$ и $k = 3$, следовательно, вероятность угадать пароль:

$$P_g = \left(\frac{1}{81} * \frac{1}{80}\right)^3 \cong 3,675 * 10^{-12},$$

или $3,675 * 10^{-10}$%.

Изначально злоумышленник даже не знает, сколько парольных изображений необходимо ввести для авторизации. Конечно, если он сможет длительное время наблюдать за монитором пользователя, есть вероятность угадать такой довольно-таки простой алгоритм.

Но надо понимать, что, используя те же идеи, можно добиться более сложных путей, объясняющих пользователю, куда кликать: за счет

Лариса Владимировна Любимова,
ведущий инженер
Тел.: (916)128-23-98
Эл. почта: lv.lyubimova@gmail.com
ОАО «НИИАС»
http://www.vniias.ru/

Larisa V. Lyubimova,
Lead engineer
Tel.: (916)128-23-98
E-mail: lv.lyubimova@gmail.com
JSC «NIIAS»
http://www.vniias.ru/

увеличения числа парольных изображений, схемы аутентификации или количества изображений, которые отображаются одновременно. Или же можно вообще избежать ситуации, при которой пользователю необходимо нажимать на изображения вовсе. Один из возможных вариантов рассмотрен во втором примере.

Пример 2. «Количество клеток»

На экране для ввода пароля в произвольном порядке разбросаны картинки. Суть метода заключается в том, что пользователь должен мысленно посчитать кратчайший путь между тремя парольными изображениями и ввести полученное число в форму. Алгоритм данного метода показан на рис. 4, пример – на рис. 5. Считать «клетки» необходимо по часовой стрелке (вверх – вправо – вниз – влево).

Для уменьшения вероятности случайного подбора пароля его ввод необходимо произвести 3 раза. Авторизация считается успешной, если пользователь не допустил ни одной ошибки.

Плюсы данного метода заключаются в том, что пользователю не нужно нажимать на изображения, а полученный результат всегда разный, так как картинки располагаются в произвольном порядке.

Предположим, что злоумышленник знает метод аутентификации. Тогда рассчитаем возможность угадать правильный пароль (число). Пусть n – количество парольных изображений по вертикали, k – по горизонтали. В нашем случае $n = k = 9$. Тогда минимальное число, которое может быть введено, $t_1 = 3$, максимальное $t_2 = 2 * n + (k-2) - 1 \equiv$ $\equiv 3 * n - 3 = 3 * (n - 1)$. При $n = 9$, $t_2 = 24$. Тогда

$$P_g = \frac{1}{t_2 - t_1} = \frac{1}{24 - 3} \cong 0,047619$$

Для успешного входа пароль необходимо ввести три раза, поэтому суммарная вероятность $P_{gf} = P_g^3 = 0,000108$, или $1,08 * 10^{-2}\%$.

Данная вероятность, конечно, выше, чем в первом способе, но и получить данные о методе аутентификации, наблюдая за пользователем, злоумышленник не может. А при увеличении количества изображений, например, до 121 ($n = 11$), вероятность угадать пароль будет $3,704 * 10^{-3}\%$.

Конечно, можно применять и совсем «специфические методы». Особенно если это позволяет уровень подготовки пользователей.

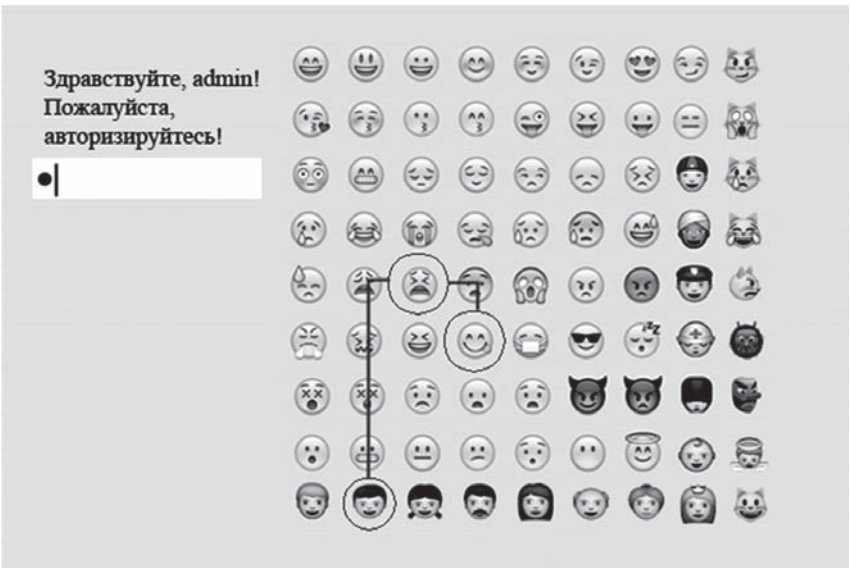


Рис. 5. *Метод «количество клеток»*

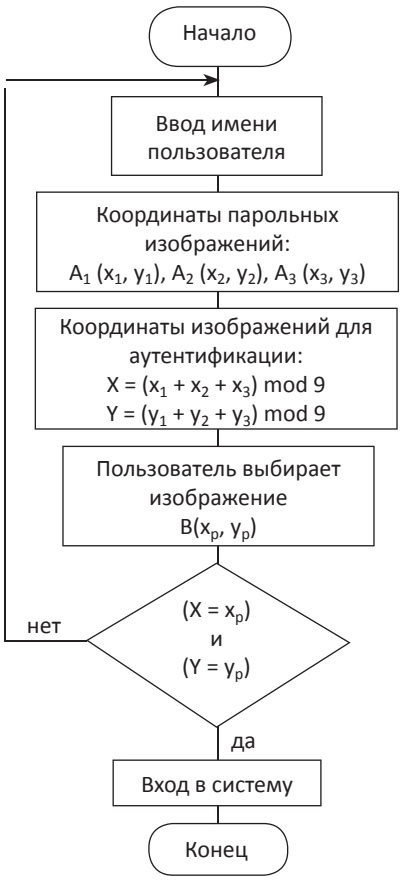


Рис. 4. *Схема аутентификации методом «количество клеток»*

Пример 3. «Модуль координат»

Данный способ будет сложен для пользователей, и вряд ли его

рационально использовать в реальной системе. Есть множество изображений, из которых три парольные. Пользователь должен мысленно наложить на картинку оси координат и сложив по модулю n (n – размерность системы) координаты парольных изображений вычислить текущий пароль. Алгоритм данного метода показан на рис. 6, пример – на рис. 7.

Красными кружками выделены парольные изображения пользователя. Их координаты соответственно: (0; 2), (7; 5) и (8; 5). Тогда координаты изображения для аутентификации:

$X = (0 + 7 + 8) \bmod 9 = 6,$

$Y = (2 + 5 + 5) \bmod 9 = 3.$

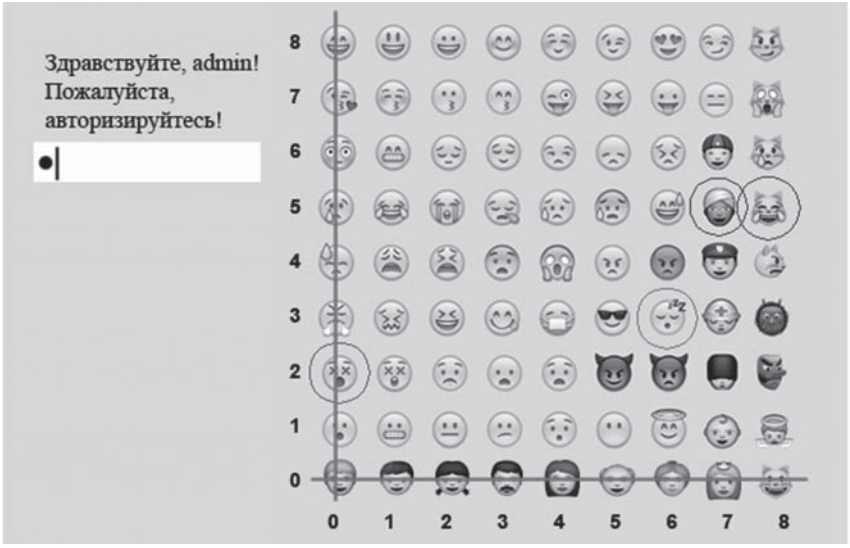


Рис. 7. *Метод «модуль координат»*

Рис. 6. *Схема аутентификации методом «модуль координат»*

Изображение для аутентификации выделено зелёным кружком. Вероятность угадать данный пароль:

$$P_g = \frac{1}{n^2} = \frac{1}{81} = 0,01234,$$

или 1,2%. При трёхкратном повторении ввода пароля: $1,88 * 10^{-4}$%, а если при этом $n = 11$, то $5,64 * 10^{-5}$%. Но если злоумышленнику неизвестен метод аутентификации, то он даже не знает, сколько изображений необходимо выбирать для входа в систему.

Заключение

Тот факт, что количество способов графической аутентификации велико, исключает возможность составления словарей подбора – ведь и сами парольные изображения можно использовать различные даже для одного метода. Вопросы же аудита, передачи парольного хэша по сети ничем не отличаются от реализации при работе с обычными буквенно-цифровыми паролями.

Главные вопросы и проблемы динамической графической аутентификации лежат в организационной сфере. Кроме того, что пользователю необходимо объяснить необходимость использования такого типа паролей, ему нужно объяснить применяемый метод. И сделать это нужно не по сети (потому что сообщение может быть перехвачено, пользователь может оставить описание метода на компьютере, в конце концов, просто не понять схему аутентификации).

Решить данную проблему можно, например, выдавая схему аутентификации «на руки». Так, как выдаются банковские карточки с пин-кодом. Это не подойдёт для интернет-ресурсов, зато вполне реализуемо в рамках предприятия (или в случаях интернет-банкинга, мобильных личных кабинетов).

Графические пароли – это попытка разработать нововведение в безопасности, принимая во внимание особенности восприятия людей. Они могут стать перспективной альтернативой обычным буквенно-цифровым паролям. Развивая математический аппарат и решая организационные вопросы, можно добиться использования предложенных методов для обеспечения надёжной и удобной пользователю системы аутентификации, как на мобильных и планшетных устройствах, так и на обычных персональных компьютерах.

Литература

1. *Афанасьев А.А., Веденьев Л.Т., Воронцов А.А. и др*. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам / А.А. Афанасьев, Л.Т. Веденьев, А.А. Воронцов, Э.Р. Газизова, А.Л. Додохов, А.В. Крячков, О.Ю. Полянская, А.Г. Сабанов, М.А. Скида, С.Н. Халяпин, А.А. Шелупанов. – М.: Горячая линия – Телеком, 2012. – 550 с.

2. *Бондарь Д.* Как построить эффективную систему управления доступом [Электронный ресурс] // Jet Info. – 2014. – № 3, апрель. – Режим доступа: http://www.jetinfo.ru/jetinfo_arhiv/entsiklopediya-idm/kak-postroit-effektivnuyu-sistemu-upravleniya-dostupom/2014