УДК 004.056.52

И. С. Ельцов, студент
А. Ю. Вдовин, канд. техн. наук, доц.
E-mail: vt@istu.ru
Ижевский государственный технический университет имени М. Т. Калашникова

Исследование «графического пароля» с использованием аутентификации на основе модели «рукопожатия» для мобильных устройств

Широко применяемая парольная аутентификация имеет многочисленные недостатки, альтернативой ей могут служить «графические пароли», некоторые из которых реализуют аутентификацию на основе модели «рукопожатия». В настоящей работе проведены исследования алгоритма, основанного на идеях Собрадо и Бирджета, применительно к небольшим экранам мобильных устройств.

Ключевые слова: «графический пароль», аутентификация на основе модели «рукопожатия», парольная аутентификация, мобильное устройство.

Введение

Аутентификация пользователей является одним из основных способов защиты от несанкционированного доступа к информации в разнообразных компьютерных системах наряду с идентификацией и авторизацией пользователей и аудитом безопасности [1].

Несмотря на большое разнообразие методов аутентификации, наиболее широко используется традиционная парольная аутентификация. Вероятно, это объясняется простотой реализации такого метода, удобством использования в мобильных приложениях. При этом парольная аутентификация имеет множество недостатков: наличие развитых методов и средств организации атак, высокую вероятность нарушения пользователями правил выбора и использования пароля (человеческий фактор). Более того, парольная аутентификация имеет принципиальную слабость, обусловленную наличием двух взаимоисключающих правил для выбора пароля: удобство для пользователей (простота запоминания) и сложность подбора злоумышленником.

В связи с этим за рубежом активно ведутся исследования по поиску методов аутентификации, способных, при определенных условиях, заменить парольную аутентификацию. К числу таких методов относятся

так называемые «графические пароли» [2–4], некоторые из них предполагают аутентификацию на основе модели «рукопожатия».

Постановка задачи

Аутентификация на основе модели «рукопожатия» во многом способна решить описанные проблемы парольной аутентификации. В соответствии с этой моделью пользователь U и компьютерная система S согласовывают при регистрации пользователя в системе функцию f, известную только им. Протокол аутентификации пользователя в этом случае выглядит так:

1) S: генерация случайного значения x (запроса); вычисление $f(x)$; сообщение запроса x пользователю;

2) U: вычисление отклика $f'(x)$; сообщение отклика системе;

3) S: если $f(x)$ и $f'(x)$ совпадают, то пользователь авторизуется в системе, иначе попытка входа в систему отклоняется.

При этом функция f должна быть такой, чтобы нарушитель по известным ему запросу x и отклику $f(x)$ не мог определить f [1].

Преимущества аутентификации на основе модели «рукопожатия» перед парольной аутентификацией обусловлены тем, что между пользователем и системой не передается никакой конфиденциальной информации, более того, даже использование внедренного на устройство пользователя вредоносного программного обеспечения (клавиатурного перехватчика или программы, перехватывающей и сохраняющей содержимое экрана) даст злоумышленнику чрезвычайно мало информации.

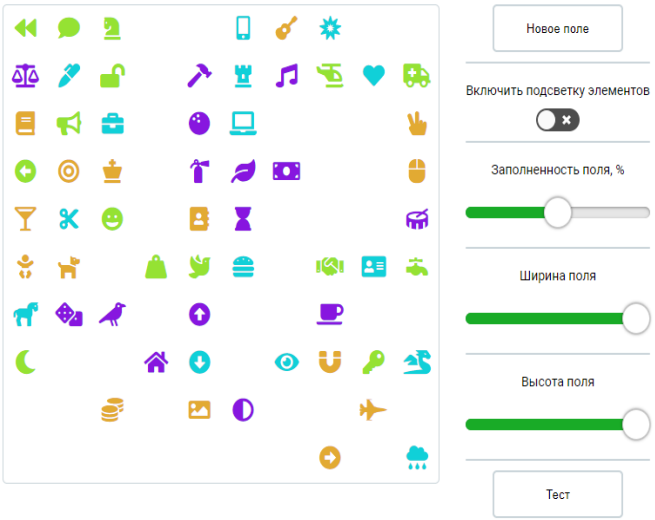
К недостаткам аутентификации на основе модели «рукопожатия» относится большая длительность этой процедуры по сравнению с парольной аутентификацией.

Один из вариантов «графического пароля» с использованием аутентификации на основе модели «рукопожатия» предложен Собрадо и Бирджетом [5]. Идея основана на том, что пользователь должен обнаружить на экране среди большого числа изображений, входящих в набор из N, три объекта, входящие в набор из k объектов, согласованный с системой на этапе регистрации (в данном случае функция f определяется этим набором) и осуществить «клик» внутри треугольника с вершинами, соответствующими этим объектам. При каждом входе в систему процесс повторяется m раз (раундов аутентификации). Авторами идеи показано, что уже при $N = 1000$ и $k = 10$ единственно возможный вид атаки (атака с исчерпывающим поиском) становится физически неосуществимым.

Целью настоящей работы является исследование возможности использования подобных алгоритмов на экранах малого размера (например, у смартфонов), где процесс аутентификации при размещении на поле большого числа изображений может быть весьма неудобным для пользователя.

Описание эксперимента

В ходе работы было создано веб-приложение, основанное на идее «графического пароля», предложенной Собрадо и Бирджетом, и позволяющее провести исследование работы алгоритма с различными параметрами. Интерфейс программы представлен на рисунке.



Интерфейс созданного веб-приложения

Приложение обладает следующими возможностями:

1) генерация нового поля аутентификации (заполнение поля изображениями из набора N случайным образом, при этом на экране будут присутствовать 3 изображения из набора k) при нажатии на кнопку «Новое поле»; необходимо отметить, что в приложении реализованы некоторые модификации канонического алгоритма, в частности, такая: если при генерации поля площадь искомого треугольника не укладывается в диапазон от 5 до 10 % общей площади поля, то генерация поля осуществляется заново;

2) изменение исходных параметров: коэффициента заполненности поля (имеется возможность менять заполненность в диапазоне от 20 до 60 %), изменение ширины и высоты поля (имеется возможность изменять каждое из значений в диапазоне от 5 до 10 клеток);

3) расчёт средней вероятности случайной авторизации злоумышленником в одном раунде. При нажатии на кнопку «Тест» отдельная функция запрашивает число испытаний n, а затем n раз генерирует новое поле и эмулирует «клик» в центре поля (вероятность принадлежности точки ключевой области увеличивается с приближением к центру экрана [6]). Затем выводится средняя по n испытаний вероятность попадания в сгенерированный треугольник для заданных параметров поля.

При этом необходимо уточнить, что диапазоны изменения параметров поля были изначально существенно ограничены, например, размер поля был ограничен квадратом с длиной стороны в 10 клеток. Подобные ограничения обусловлены необходимостью компромисса между минимально допустимой сложностью подбора функции аутентификации злоумышленником и максимально допустимой величиной времени, затрачиваемого пользователем на процесс аутентификации. В связи с этим были выбраны указанные границы диапазонов всех параметров, при этом учитывались и ограничения, накладываемые размерами экрана конечного устройства (например, смартфона).

Выясним оптимальный размер поля аутентификации, коэффициент заполненности и соотношение сторон. Исследования проводились по общему алгоритму:

1) поле многократно (для минимизации влияния случайных исходов на общий результат было выбрано $n = 1000000$) заполняется изображениями из набора N случайным образом, при этом к ним добавляются 3 изображения из k;

2) эмулируется клик в случайную точку поля, затем проверяется, было ли осуществлено попадание в искомый треугольник.

Результаты и их обсуждение

Сначала исследуем зависимость соотношения сторон поля аутентификации и вероятности случайно попасть в искомую область. Для $k = 3$, $N = 60$ результаты при различных размерах поля приведены в табл. 1.

Здесь во всех случаях коэффициент заполненности равнялся 60 % (максимально возможное из имеющихся значений).

Можно сделать вывод, что оптимальной формой поля является квадрат. При сравнении прямоугольников с разными длинами сторон видно, что при сопоставимых площадях вероятности того, что центр поля принадлежит искомому треугольнику, существенно различаются. Напри-

мер, для прямоугольников 8×8 и 6×10 вероятности различаются более чем в три раза (0,09 и 0,297 соответственно), а для прямоугольников 6×6 и 5×7 – почти в три раза (0,1 и 0,299 соответственно).

Таблица 1. **Вероятность случайной авторизации злоумышленником в одном раунде при различных размерах поля**

Ширина поля, число клеток	Высота поля, число клеток					
	10	9	8	7	6	5
10	0,089					
9	0,143	0,099				
8	0,196	0,148	0,092			
7	0,241	0,240	0,162	0,106		
6	0,297	0,255	0,220	0,191	0,100	
5	0,337	0,359	0,316	0,299	0,218	0,145

Исследуем влияние коэффициента заполненности на вероятность определения злоумышленником изображений, входящих в k (вообще, очевидно, что задача злоумышленника тем сложнее, чем большее число изображений на экране будет присутствовать, но попытаемся оценить, насколько она усложнится при том или ином увеличении коэффициента заполненности).

Зададим начальные условия $N = 120$, $k = 6$, $m = 10$; при этом для коэффициента заполненности в 60 % на экране будут присутствовать 60 изображений (из них 57 из набора N, и 3 – из набора k).

Для проверки была разработана функция, реализующая сценарий атаки злоумышленника. Эмулируется проведение заданного числа раундов аутентификации, при этом в первом раунде сохраняет комбинации из трех изображений, которые потенциально могут составлять парольную последовательность, а в следующих раундах из сохраненного перечня отбрасываются неудовлетворительные комбинации. Затем возвращается число возможных оставшихся комбинаций. Описанный алгоритм повторялся 10 раз, после чего вычислялось среднее арифметическое и округлялось до ближайшего целого. При этом в каждом случае эмулируется «клик» пользователем в центр масс треугольника.

По результатам, приведённым в табл. 2, можно отметить следующую закономерность – после 1 раунда имеем спад, более или менее резкий, в зависимости от коэффициента заполненности, а затем результат колеблется в некоторых пределах, не имея тенденции к стабильному росту или спаду. Это позволяет с высокой вероятностью утверждать, что в пределах 5–10 раундов аутентификации злоумышленник не сможет точно определить искомый набор изображений. При этом необходимо отметить, что даже небольшое увеличение коэффициента заполненно-

сти (например, с 20 % до 30 % приводит к увеличению числа возможных комбинаций для злоумышленника в 2 раза и более).

Таблица 2. **Количество возможных вариантов для злоумышленника при изменении коэффициента заполненности**

№ раунда	Коэффициент заполненности, %				
	20	30	40	50	60
1	345	624	1849	3648	4510
2	134	529	1648	1894	4377
3	147	579	1099	2049	3324
4	145	487	1019	1525	3919
5	134	289	926	1970	4347
6	126	600	1419	2222	3545
7	131	548	1164	2546	3454
8	155	471	1285	2213	3872
9	127	555	1218	1760	4172
10	155	488	1027	1959	4354

Кроме того, было проведено исследование на добровольцах для оценки необходимого времени аутентификации. Тестирование проводилось следующим образом: каждый испытуемый в течение нескольких минут (5–10) тренировался использовать приложение при различных параметрах алгоритма, затем проводились 10 раундов аутентификации, общее время аутентификации фиксировалось в консоли браузера, после чего вычислялось среднее время одного раунда. Тестирование проводилось для поля 10×10 клеток с коэффициентом заполненности от 20 % до 60 %.

Результаты исследования сведены в табл. 3.

Таблица 3. **Оценка времени, необходимого для аутентификации**

Коэффициент заполненности, %	Время одного раунда аутентификации, с			
	Испытуемый 1	Испытуемый 2	Испытуемый 3	Среднее
20	10,1	10,8	12,2	11,0
30	12,3	10,7	13,5	12,2
40	14,4	11,3	16,1	13,9
50	17,6	12,8	17,0	15,8
60	19,7	13,1	18,9	17,2

Таким образом, даже при 5–6 раундах аутентификации общее затраченное пользователем время может составлять примерно две минуты, что в десятки раз превышает время аутентификации, например, с помо-

щью PIN-кода. Отчасти это можно объяснить новизной алгоритма для испытуемых.

Выводы

Проведенные исследования позволяют сделать следующие выводы. Оптимальной формой поля аутентификации является квадрат. В заданном диапазоне значений оптимальная величина коэффициента заполненности – 60 % (при этом значении коэффициента задача злоумышленника может усложниться в два раза и более по сравнению с вариантом использования коэффициента заполненности в 50 %). Несмотря на существенную величину времени аутентификации исследуемого алгоритма применительно к мобильным устройствам с небольшим экраном, в некоторых случаях это может быть оправдано, так как применение подобного алгоритма позволяет решить проблему «подглядывания» при вводе пароля и существенно усложнить проведение атак злоумышленником даже при использовании им специальных программ.

Список литературы

1. *Хорев, П. Б.* Программно-аппаратная защита информации / П. Б. Хорев. – Москва : ФОРУМ, 2013. – 352 с.

2. *Blonder, G.* Graphical passwords. United States Patent, 1996, 5, 559, 961.

3. *Dhamija, R., Perrig*, *A.* Deja vu: a user study using images for authentication // Proceedings of 9th USENIX Security Symposium (August 14-17, 2000). Denver, USA : USENIX, 2000. URL: https://www.usenix.org/legacy/publications/library/proceedings/sec2000/full_papers/dhamija/dhamija.pdf.

4. *Suo, X., Zhu, Y., Owen, G. S.* Graphical passwords: a survey // 21st Annual Computer Security Applications Conference (ACSAC'05). Tucson, USA : IEEE. DOI: 10.1109/CSAC.2005.27.

5. *Sobrado, L., Birget*, *J.-C.* Graphical passwords // The Rutgers Scholar. An Electronic Bulletin for Undergraduate Research. 2002. Vol. 4. URL: https://rutgersscholar.libraries.rutgers.edu/volume04/sobrbirg/sobrbirg.htm.

6. *Минаков, В. А.* Анализ эффективности аутентификации с помощью графических паролей / В. А. Минаков // Вестник Воронежского государственного технического университета. – 2009. – Т. 5, № 11. – С. 228–230.

I. S. El'tsov, student
A. Yu. Vdovin, CSc in engineering, associate professor
E-mail: vt@istu.ru
Kalashnikov Izhevsk State Technical University, Izhevsk, Russian Federation

Research of the "Graphical Password" Using Challenge Response Authentication for Mobile Devices

Widely used password authentication has numerous disadvantages. An alternative is "graphical password", some of which implement challenge response authentication. In this paper, the algorithm based on the ideas of Sobrado and Birget is studied in relation to small screens of mobile devices.

Keywords: graphical password, challenge response authentication, password authentication, mobile device.