УДК 004.056.53 **DOI: 10.18413/2518-1092-2020-5-2-0-4**

Какаев Д.В.
Девицына С.Н.

СОВЕРШЕНСТВОВАНИЕ МЕТОДА ГРАФИЧЕСКОЙ АУТЕНТИФИКАЦИИ ДЛЯ ЗАЩИТЫ ОТ «ПЛЕЧЕВОГО СЕРФИНГА»

Севастопольский государственный университет, ул. Университетская, д. 33, г. Севастополь, 299053, Россия

e-mail: 619deniss61999@gmail.com, sndevitsyna@sevsu.ru

Аннотация
В статье представлен пример реализации графической аутентификации пользователей на основе схемы треугольника. Актуальность исследования обусловлена необходимостью защиты вводимых пользователем идентификаторов от плечевого серфинга. Проблема защиты от подглядывания при вводе идентификаторов, например, паролей, пин-кодов, символов CAPTCHA (капча) возникает из-за того, что некоторые информационные системы находятся в помещениях с большим количеством людей. Наиболее часто такими системами являются терминалы и банкоматы. При этом подглядывание становится методом кражи парольной информации, и широко используется злоумышленником. Одним из решений данной проблемы является использование графической аутентификации с защитой от подглядываний. На данный момент нет надежных модулей графической аутентификации, исключающих возможность подглядывания парольной информации. Стандартные алгоритмы реализации схем графической аутентификации с защитой от плечевого серфинга имеют ряд проблем с безопасностью и удобством эксплуатации. Предложенный метод обеспечивает достаточную защищенность и исключает попытки взлома, даже при наблюдении злоумышленником за прохождением графической аутентификации. В статье представлено описание нового подхода к проведению графической аутентификации на основе схемы треугольника. Описаны результаты тестирования приложения на реальных пользователях. На основе статистики входа и опроса участников сделаны выводы о результатах работы приложения.
Ключевые слова: аутентификация; информационная система; Linux-PAM; графическая аутентификация; брутфорс.

UDC 004.056.53

Kakaev D.V.
Devitsyna S.N.

IMPROVED GRAPHICAL AUTHENTICATION ALGORITHM WITH ANTI-SPYING PROTECTION

Sevastopol state University, 33 Universitetskaya St., Sevastopol, 299053, Russia

e-mail: 619deniss61999@gmail.com, sndevitsyna@sevsu.ru

Abstract
This article provides an example of implementing graphical user authentication based on a triangle scheme. The relevance of the research is due to the need to protect user-entered identifiers from shoulder surfing. The problem of protection against spying when entering identifiers, such as passwords, pin codes, CAPTCHA characters, occurs because some information systems are located in rooms with a large number of people. The most common such systems are terminals and ATMs. In this case, peeping becomes a method of stealing password information, and is widely used by an attacker. One solution to this problem is to use graphical authentication with anti-peeping protection. At the moment, there are no reliable graphical authentication modules that exclude the possibility of spying on password information. Standard algorithms for implementing graphical authentication schemes with protection from shoulder surfing have a number of problems with security and usability. The proposed method provides sufficient security and eliminates hacking attempts, even if the attacker observes the passage of

graphical authentication. The article presents the description of a new approach to graphical authentication based on the schema of the triangle. The results of testing the app on real users are described. Based on login statistics and a survey of participants, conclusions are made about the results of the application.
Keywords: authentication; information system; Linux-PAM; graphical authentication; brutforce.

ВВЕДЕНИЕ

В настоящее время остро стоит вопрос обеспечения безопасности конфиденциальной информации, которая хранится в информационных системах. Перед началом работы с любой системой пользователь должен пройти процедуру авторизации. В процессе прохождения процедуры пользователь предоставляет системе определенный, заранее установленный набор идентификаторов, по которым система убеждается, что данный пользователь тот, за кого себя выдает, и предоставляет ему полномочия по использованию контента, либо выполнению каких-то действий.

Перед разработчиками информационных систем стоит задача создания безопасной и удобной системы авторизации. Поэтому постоянно создаются новые методы аутентификации и модернизируются уже известные методы. Создание систем аутентификации является актуальным направлением работы и будет таким оставаться до тех пор, пока актуальна аутентификация, как метод защиты информационных систем.

Некоторые информационные системы находятся в местах с большим количеством людей. Для таких систем актуально подглядывание, как метод кражи парольной информации. Одним из решений данной проблемы является использование графической аутентификации с защитой от подглядываний [Жук, А.П, 2018; Акушуев, Р.Т., 2020].

ОСНОВНАЯ ЧАСТЬ

Существуют три схемы графической аутентификации с защитой от плечевого серфинга: схема треугольника, схема диагоналей четырехугольника, схема подвижной рамки. В основе всех схем лежит один механизм. Отличием является только метод определения правильности введенного пароля. Проведено сравнение указанных схем, результаты представлены в табл. 1.

Таблица 1

Сравнение схем графической аутентификации с защитой от плечевого серфинга

Table 1

Comparison of graphical authentication algorithm with anti-spying protection

Схема	Удобство		Безопасность			
	Среднее время, с	Процент правильных входов, %	Анализ частот	Полный перебор	Вход на удачу	Оптимизированный перебор
Треугольника	25	91,8	+	+	+	+
Диагоналей	33	78,2	+	+	+	+
Подвижной рамки	37	99,5	+	+	+	+

Как видно из сравнения, для всех схем актуальны одинаковые проблемы с безопасностью, но по удобству схема треугольника является лучшей. Поэтому принято решение разработать программу, использующую данный метод с лучшими показателями безопасности и удобства эксплуатации пользователем [Studbooks, 2020; Habr, 2011].

Был произведен анализ изменений показателей удобства и безопасности в зависимости от изменений параметров схемы, и получены оптимальные параметры:

- общее количество изображений (*n*): 400;
- количество парольных изображений (*k*): 5;
- размер сгенерированного изображения: 13×13 изображений;
- количество повторений: 7.

Изменение параметров безопасности представлено в табл. 2.

Таблица 2

Зависимость возможных комбинаций пароля от общего количества изображений и количества парольных изображений

Table 2

Dependence of possible password combinations on the total number of images and the number of password images

k \ n	**300**	**350**	**400**	**450**	**500**	**Символьный**
4	$0{,}3*10^9$	$0{,}6*10^9$	$1*10^9$	$1{,}7*10^9$	$2{,}5*10^9$	$0{,}049*10^9$
5	$19*10^9$	$42*10^9$	$83*10^9$	$150*10^9$	$255*10^9$	$4{,}1*10^9$
6	$0.96*10^{12}$	$2{,}4*10^{12}$	$5{,}4*10^{12}$	$11{,}1*10^{12}$	$21*10^{12}$	$0{,}351*10^{12}$

Как видно из табл. 2, увеличение общего количества изображений дает небольшой прирост возможных комбинаций пароля. Тем более бесконечно увеличивать общее количество изображений не получится, так как изображения должны быть абсолютно разными и непохожими. Увеличение длины пароля значительно увеличивает количество возможных комбинаций. Но с запоминанием длинных паролей у пользователей могут возникнуть проблемы, поэтому была выбрана оптимальная длина. В то же время любой графический пароль будет лучше аналогичного по длине буквенно-символьного пароля. Кроме того, большинство пользователей используют в качестве пароля не случайные наборы символов [Kaspersky, 2019].

Общий принцип работы аутентификации на основе схемы треугольника можно описать следующим образом. Сначала пользователь проходит регистрацию. На этом этапе необходимо из представленных 400 изображений выбрать 5. К данному набору изображений выдвигается ряд требований, таких, что все изображения должны быть абсолютно разными, чтобы пользователь легко запоминал и не возникало проблем с узнаванием.

Потом пользователь проходит аутентификацию. На этом этапе пользователь предъявляет идентификатор, который может быть логином или смарт-картой. Если такой пользователь существует, то на сервере генерируется случайный набор из 169 изображений, на котором присутствуют 3 из 5 парольных изображений (рис. 1). На сгенерированном изображении пользователь мысленно находит свои парольные изображения, и мысленно строит треугольник, вершинами которого являются центры парольных изображений, и кликает внутри данного треугольника. Важным требованием является запрет на поиск парольных изображений курсором или последовательные клики на эти изображения, чтобы помешать злоумышленнику выяснить пароль [Kaspersky, 2019].

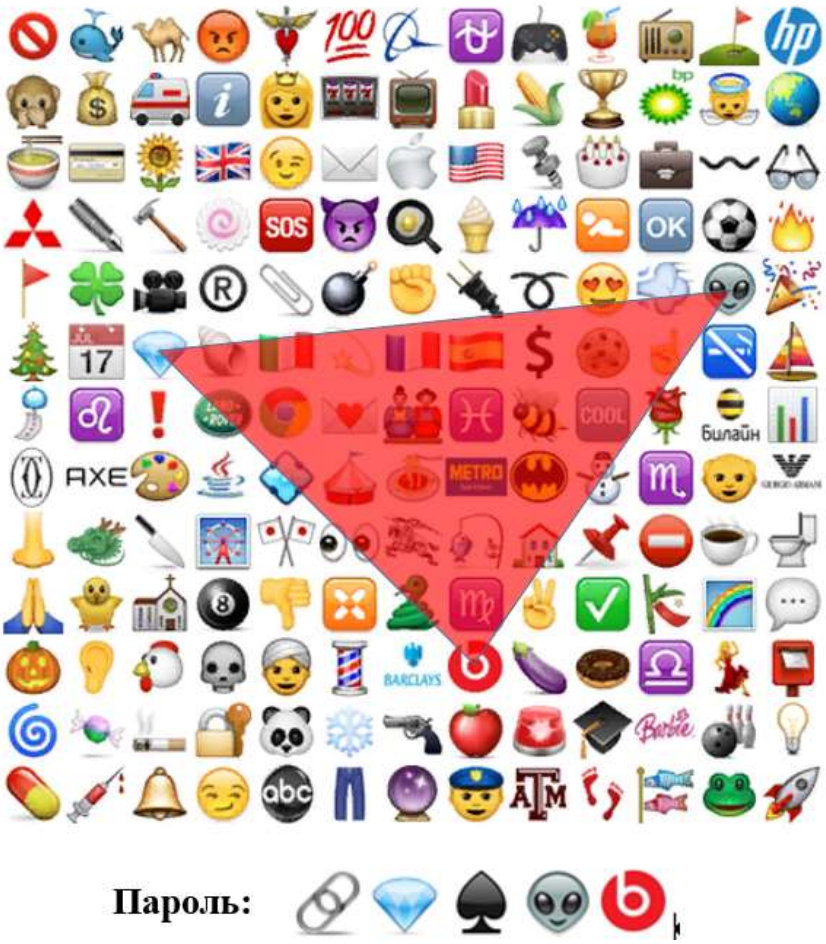

Рис. 1. Пример сгенерированного изображения
Fig. 1. Example of the generated image

На рис. 1 красным выделена зона, в которой пользователь может совершить клик, считающийся правильным при указанном ниже пароле. В реальном сгенерированном изображении пароль будет отсутствовать. Данную операцию пользователю необходимо совершить правильно подряд семь раз, чтобы уменьшить возможность войти в аккаунт случайным образом.

Проведено сравнение данного метода с аналогами [Будко, Е.Г., 2011; IBM, 2009]. Существует Linux-PAM (Pluggable Authentication Modules) подключаемый модуль аутентификации для операционной системы Linux. В данном модуле реализована схема треугольника и диагоналей четырехугольника. Но данный модуль используется только для защиты входа в систему или для защиты установленных на компьютер приложений. К тому же у реализации схем имеется ряд проблем с безопасностью и удобством, которые возможно исправить.

Проблему узкого круга применения данного модуля можно решить путем разработки нового веб-приложения. В таком веб-приложении все вычисления и пароли будут храниться на сервере, что исключит возможность кражи и взлома пароля перебором удаленно, как это могло быть в Linux [Будко Е.Г., 2011].

Также проведен анализ частоты попадания конкретных изображений в сгенерированный набор PAM-модуля. Поскольку главным принципом данного приложения является защита от подглядываний, то можно предположить, что злоумышленник имеет сгенерированные изображения и клики пользователя. Имея менее 100 сгенерированных изображений, злоумышленник может однозначно определить все парольные изображения (рис. 2). Для этого был написан скрипт, имитирующий генерацию случайных наборов изображений.

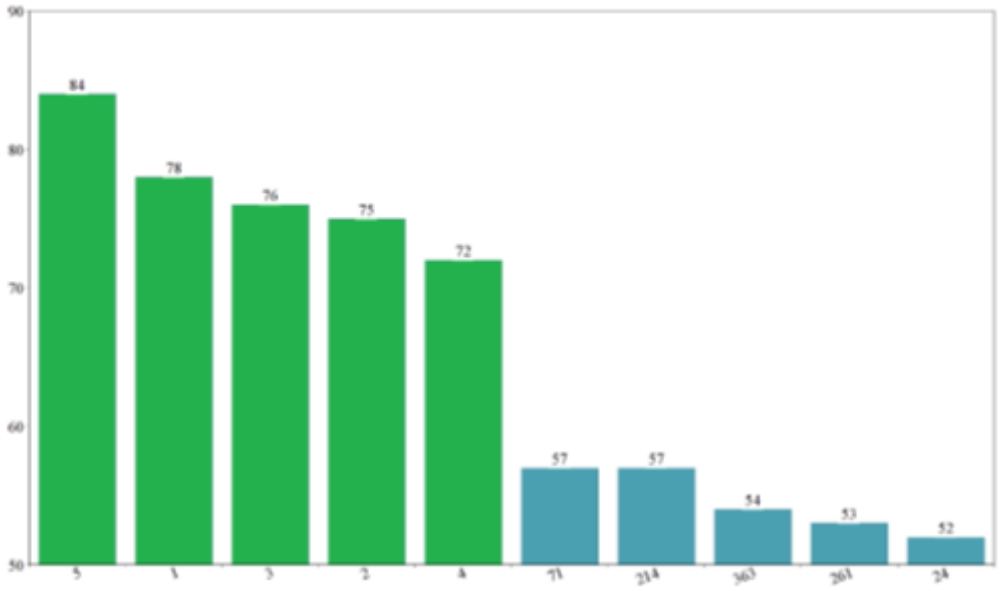

Рис. 2. Частота попадания изображений в сгенерированное
Fig. 2. Frequency of images entering the generated image

На рис. 2 парольные изображения сразу выделяются. Их частота попадания намного выше, чем у всех других изображений. Злоумышленник сможет без проблем разгадать пароль, наблюдая за несколькими успешными процедурами входа [IBM, 2009].

Для устранения данной уязвимости можно для каждого пользователя генерировать случайный набор из 15-20 изображений, у которых будет более высокая вероятность попадания в сгенерированное изображение. Эта вероятность может случайно выбираться и быть в 2-3 раза выше вероятности попадания в остальные изображения. Данное усовершенствование значительно усложнит анализ частот попадания изображений (рис. 3).

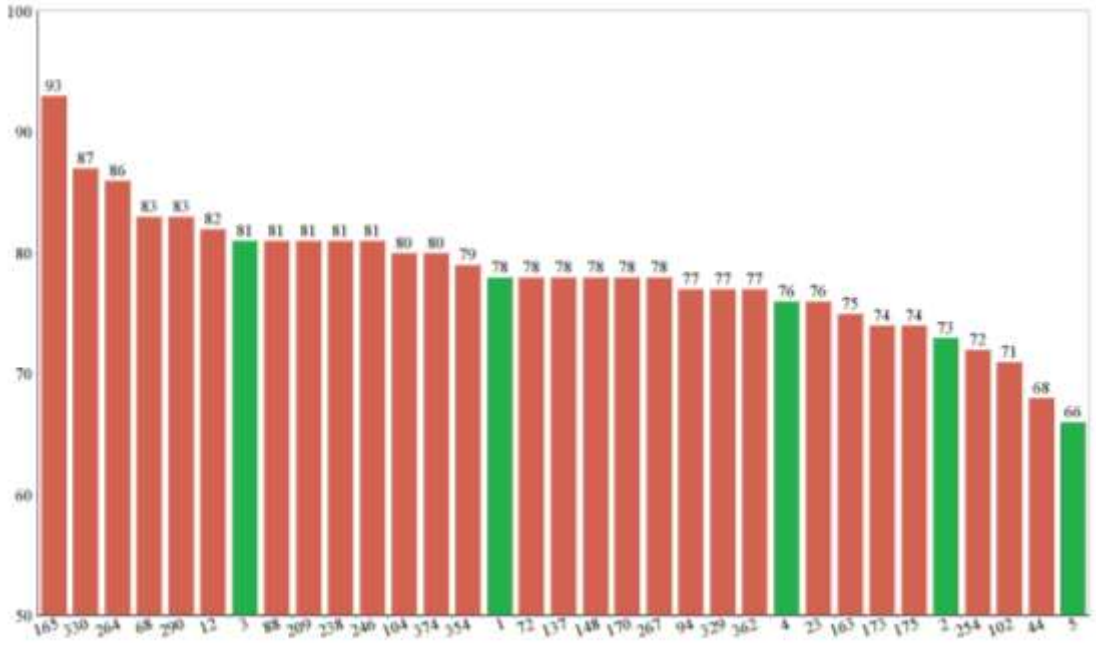

Рис. 3. Частота попадания изображений после изменений
Fig. 3. Frequency of contact with the images after the changes

Теперь парольные изображения равномерно расположены среди других изображений и никак не выделяются среди прочих. Обладая даже сведениями о 10 000 процедурах входа, злоумышленник не сможет однозначно определить пароль.

В аналоговом модуле нет ограничений на генерируемый треугольник. Таким образом треугольник может быть слишком большим, что увеличивает вероятность взлома кликом наудачу, или слишком маленьким, что увеличивает время поиска парольных изображений и увеличивает процент ошибочных кликов. Для улучшения данных показателей необходимо на момент генерации изображений сделать проверку площади сгенерированного треугольника. Она должна быть 5-35% от общей площади изображения.

Поскольку злоумышленник может иметь набор сгенерированных изображений и координат клика на них, он может провести анализ положения изображений относительно кликов. Разработать такой алгоритм достаточно сложно, но возможно. Поэтому необходимо создать защиту от подобного вида взлома. Для этого случайным образом с небольшой вероятностью может быть сгенерировано специальное изображение, на котором отсутствуют одно или несколько из трех парольных изображений. Таким образом, пользователь не сможет построить треугольник. В таком случае пользователю необходимо кликнуть в любом месте, и клик будет засчитан правильным. Данное решение значительно помешает злоумышленнику анализировать результаты, ведь злоумышленнику не известно – когда пользователь кликнул в случайном месте.

В PAM-модуле пароль хранится на компьютере в зашифрованном виде, но он может быть украден и взломан перебором. Для разработанного приложения это не актуально, но все же приложение может быть подвержено атаке перебором. Защититься от этого можно установкой задержки между процедурами входа, после превышения установленного количества ложных кликов. Также вместо задержки может быть прислана капча или заблокирован на время данный IP. А при превышении следующего порога аккаунт пользователя может подвергаться временной блокировке. Таким образом, любая атака перебором становится неактуальна [Hackware, 2017; Somemoreinfo, 2016].

Таким образом, были устранены проблемы с безопасностью и повышено удобство использования системы аутентификации. Количество комбинаций для полного перебора $83 \cdot 10^9$, не актуально из-за защиты от перебора. Взлом кликом наудачу: вероятность успешно войти равна 0,0013, это – не актуально из-за защиты от перебора. Анализ частот выпадения: невозможен при наличии 10 000 сессий входа, не актуален. Оптимизация перебора: значительно усложнена из-за специальных сгенерированных изображений. Данная угроза остается еще актуальной, но вероятность успешной реализации уменьшена.

Для оценивания удобства эксплуатации метод был апробирован с привлечением 40 участников, каждому из которых было предложено пройти процедуру аутентификации. Изменения алгоритма проведения аутентификации повлияли на удобство эксплуатации системы. Так, время прохождения одной процедуры составило 21 с вместо 25 с. Количество правильных кликов относительно ошибочных составило 93,5 % вместо 91,8 %.

ЗАКЛЮЧЕНИЕ

Изложенный в статье подход был разработан Какаевым Д.В. в выпускной квалификационной работе. В результате был усовершенствован механизм графической аутентификации с защитой от плечевого серфинга, повышено удобство эксплуатации и безопасность процедуры, увеличена область применения данной системы аутентификации. Все вычисления проводятся на сервере, поэтому перехват всех данных графической аутентификации не позволит злоумышленнику взломать аккаунт. Приложение проверено на тестовой группе и показало хорошие результаты.

Список литературы

1. Habr, 2011. Практические рекомендации по выбору паролей по результатам взлома antichat.ru. URL: https://habr.com/ru/post/122633. (дата обращения 08.05.2020).

2. Hackware, 2017. Брут-форс веб-сайтов: инструкция по использованию patator, Hydra, Medusa. URL: https://hackware.ru/?p=1453 (дата обращения 07.05.2020).

3. IBM, 2009. Основы и настройка PAM. URL: https://www.ibm.com/developerworks/ru/library/l-pam/ (дата обращения 08.05.2020).

4. Kaspersky, 2019. Как составить надежный пароль. URL: https://support.kaspersky.ru/common/windows/3730 (дата обращения 08.05.2020).

5. Somemoreinfo, 2016. Защита сайта от перебора пароля URL: http://somemoreinfo.ru/zashhita-sajta-ot-perebora-parolya (дата обращения 03.05.2020).

6. Studbooks, 2020. Простая схема графического пароля URL: https://studbooks.net/2410599/informatika/prostaya_shema_graficheskogo_parolya (дата обращения 01.05.2020).

7. Акушуев, Р.Т. 2020. Аутентификация и идентификация как метод защиты информации // E-SCIO, 1(40): 442-447. URL: https://elibrary.ru/item.asp?id=42500999& (дата обращения 10.05.2020).

8. Будко, Е.Г., 2011. Графическая аутентификация в Linux. URL: https://www.bibliofond.ru/view.aspx?id=607209 (дата обращения 08.05.2020).

9. Жук, А.П. и др. 2019. Защита информации. URL: https://znanium.com/catalog/product/937469 (дата обращения: 02.05.2020).

References

1. Habr, 2011. Practical recommendations for choosing passwords based on the results of hacking antichat.ru. URL: https://habr.com/ru/post/122633 (date of circulation: 08.05.2020).

2. Hackware, 2017. Brut-force websites: instructions for using patator, Hydra, Medusa. URL: https://hackware.ru/?p=1453 (date of circulation: 07.05.2020).

3. IBM. Understanding and configuring PAM. URL: https://www.ibm.com/developerworks/ru/library/l-pam (date of circulation: 08.05.2020)

4. Kaspersky. How to create a strong password. URL: https://support.kaspersky.ru/common/windows/3730 (date of circulation: 08.05.2020)

5. Somemoreinfo, 2017. Protecting the site from overwriting the URL password: http://somemoreinfo.ru/zashhita-sajta-ot-perebora-parolya (date of circulation: 03.05.2020).

6. Studbooks, 2020. A simple diagram of the graphic. URL: https://studbooks.net/2410599/informatika/prostaya_shema_graficheskogo_parolya (date of circulation: 01.05.2020).

7. Akushuev, R.T., 2020. Authentication and identification as a method of information security. E-SCIO, 1(40): 442-447. URL: https://elibrary.ru/item.asp?id=42500999& (date of circulation: 10.05.2020).

8. Budko, E.G., 2010. Graphical authentication in Linux. URL: https://www.bibliofond.ru/view.aspx?id=607209 (date of circulation: 08.05.2020).

9. ZHuk, A.P. etc. 2019. Information protection. URL: https://znanium.com/catalog/product/937469 (date of circulation: 02.05.2020).

Какаев Денис Валерьевич, студент 4 курса кафедры Информационная безопасность Института радиоэлектроники и информационной безопасности
Девицына Светлана Николаевна, кандидат технических наук, доцент, доцент кафедры Информационная безопасность Института радиоэлектроники и информационной безопасности

Kakaev Denis Valerievich, 4th year student of the Department Information security, Institute of Radioelectronics and Information security
Devitsyna Svetlana Nikolaevna, Candidate of Technical Sciences, Associate Professor, Associate Professor of the Department Information security, Institute of Radioelectronics and Information security