DOI: https://doi.org/10.15688/NBIT.jvolsu.2019.1.3

УДК 004.338
ББК 32.971.9

АНАЛИЗ СВОЙСТВ И ХАРАКТЕРИСТИК ПАРОЛЕЙ ДЛЯ АППАРАТНОГО МЕНЕДЖЕРА НА ОСНОВЕ МИКРОКОНТРОЛЛЕРА ARDUINO

Алексей Владимирович Лебеденко

Старший преподаватель кафедры информационной безопасности,
Севастопольский государственный университет
avlebedenko@sevsu.ru
ул. Университетская, 33, 299053 г. Севастополь, Российская Федерация

Евгений Сергеевич Васильев

Студент кафедры информационной безопасности,
Севастопольский государственный университет
1996vasilyev@gmail.com
ул. Университетская, 33, 299053 г. Севастополь, Российская Федерация

Аннотация. Статья посвящена пользовательской аутентификации, энтропии паролей и допустимым паролям для сайтов, методам усовершенствования аутентификации путем разработки аппаратного менеджера пароля на основе микроконтроллера Arduino.

Ключевые слова: энтропия пароля, допустимые значения пароля, алгоритм работы устройства, характеристика пароля, микроконтроллер.

Актуальность темы

На сегодняшний день использование паролей является одним из самых популярных способов аутентификации пользователей в интернете. Из-за способов хранения паролей, разработчики вынуждены накладывать ограничения на то, какие пароли безопаснее использовать. Так, например, чаще всего пароль должен содержать не менее 8 символов, иметь буквы разных регистров, содержать специальные символы и т. д. Можно констатировать, что со временем, эти ограничения только усиливаются, а это в свою очередь усложняет выбор безопасного и одновременно легко запоминаемого пароля. Так, например, наиболее безопасный пароль будет содержать 128 символов с максимальной энтропией.

Анализ паролей, используемых для аутентификации

Сложность пароля – мера оценки времени, которое необходимо затратить на угадывание пароля или подбор каким-либо методом, например, методом полного перебора. Оценка того, как много попыток (времени) в среднем потребуется взломщику для угадывания пароля. Другое определение термина – функция от длины пароля, его запутанности и непредсказуемости.

С точки зрения взлома методом полного перебора (brute-force attack) устойчивость пароля к хакерским атакам сильно зависит как от его длины, так и от используемого набора знаков. Энтропия пароля (сложность пароля, измеряемая в битах), сгенерированного случайным образом, рассчитывается по формуле [1]:

$$H = L\frac{\ln N}{\ln 2}, \qquad (1.1)$$

где L – набор символов в пароле; N – количество символов в используемом алфавите; ln – натуральный логарифм, то есть логарифм по основанию e = 2,71828.

Энтропия пароля, сгенерированного случайным образом, может изменяться с учетом используемого набора символов.

Рост общей энтропии пароля, а, следовательно, и увеличение общего количества возможных комбинаций, используемых при его составлении, зависит как от длины пароля, так и от доступного набора символов [2]. При этом общее количество возможных комбинаций пароля рассчитывается по формуле:

$$C = L^N. \qquad (1.2)$$

Пользователя все-таки больше интересует количество возможных комбинаций при более приемлемой длине пароля в диапазоне символов, которые приведены в таблице. При этом следует заметить, что уже при длине пароля в четыре знака количество возможных комбинаций для пароля, составленного из арабских цифр, латинского алфавита с регистром и со специальными символами, количество возможных комбинаций в 8 145,1 раза выше, чем для пароля, составленного только из арабских цифр. В то же время при длине пароля в 10 символов вышеуказанное превышение уже достигает 5 987 369 392,4 раза или $5{,}987 \times 10^9$ раза.

Для того чтобы создать максимально безопасный пароль, нужно определить максимально возможную длину паролей, которые можно использовать на разных ресурсах и выбрать такую, которая будет удовлетворять выбранные критерии [4]. При анализе сайтов были выявлены такие ограничения [3]:

– использование только латинских символов;

– начало и конец пароля должен состоять из буквы;

– использование только букв (A–Z и a–z) и цифр (0–9);

– использование специальных символов: !@#$%^&*()–_+=;:,./?\|‘[]{};

– длина пароля не должна быть более 30 символов.

Алгоритм работы устройства

Устройство состоит из таких элементов как: выделенная память, USB, блок ввода

Таблица

Рост количества возможных комбинаций пароля в зависимости от его длины

Количество символов в пароле, в ед.	Арабские цифры	Латинский алфавит без регистра	Арабские цифры + латинский алфавит без регистра	Латинский алфавит с регистром	Арабские цифры + латинский алфавит с регистром	Арабские цифры + латинский алфавит с регистром + спец. символы
4	10 000	456 976	1 679 616	7 311 616	14 776 336	81 450 625
5	100 000	11 881 376	60466176	$3{,}8\cdot10^{8}$	$9{,}16\cdot10^{8}$	$7{,}738\cdot10^{9}$
6	1 000 000	$3{,}089\cdot10^{8}$	$2{,}177\cdot10^{9}$	$1{,}97\cdot10^{10}$	$5{,}680\cdot10^{10}$	$7{,}351\cdot10^{11}$
7	10 000 000	$8{,}032\cdot10^{9}$	$7{,}836\cdot10^{10}$	$1{,}028\cdot10^{12}$	$3{,}522\cdot10^{12}$	$6{,}983\cdot10^{13}$
8	100 000 000	$2{,}088\cdot10^{11}$	$2{,}821\cdot10^{12}$	$5{,}346\cdot10^{13}$	$2{,}183\cdot10^{14}$	$6{,}634\cdot10^{15}$
9	1 000 000 000	$5{,}430\cdot10^{12}$	$1{,}016\cdot10^{14}$	$2{,}780\cdot10^{15}$	$1{,}354\cdot10^{16}$	$6{,}302\cdot10^{17}$
10	$1{,}000\cdot10^{10}$	$1{,}412\cdot10^{14}$	$3{,}656\cdot10^{15}$	$1{,}446\cdot10^{17}$	$8{,}393\cdot10^{17}$	$5{,}987\cdot10^{19}$
11	-	$3{,}670\cdot10^{15}$	$1{,}316\cdot10^{17}$	$7{,}517\cdot10^{18}$	$5{,}204\cdot10^{19}$	$5{,}688\cdot10^{21}$
12	-	$9{,}543\cdot10^{16}$	$4{,}738\cdot10^{18}$	$3{,}909\cdot10^{20}$	$3{,}226\cdot10^{21}$	$5{,}404\cdot10^{23}$
13	-	$2{,}481\cdot10^{18}$	$1{,}706\cdot10^{20}$	$2{,}033\cdot10^{22}$	$2{,}000\cdot10^{23}$	$5{,}133\cdot10^{25}$
14	-	$6{,}451\cdot10^{19}$	$6{,}141\cdot10^{21}$	$1{,}057\cdot10^{24}$	$1{,}240\cdot10^{25}$	$4{,}877\cdot10^{27}$
15	-	$1{,}677\cdot10^{21}$	$2{,}211\cdot10^{23}$	$5{,}496\cdot10^{25}$	$7{,}689\cdot10^{26}$	$4{,}633\cdot10^{29}$

данных, при подключении к ПК устройство определяется как HID-клавиатура, что позволяет вводить данные через блок ввода данных [5; 6].

Устройство работает по алгоритму, приведенному на рисунке.

Вначале, необходимо активировать устройство вводом PIN-кода, который представляет собой комбинацию клавиш, на клавиатуре, состоящую из 7 символов. При правильном вводе PIN-кода устройство будет активировано и затем можно будет им воспользоваться. Если PIN-код был введен неверно, то у пользователя будет еще 10 попыток, после чего устройство заблокируется на 5 минут. После активации устройства можно воспользоваться функциями создания пароля или ввода уже сохраненного пароля на устройстве.

Заключение

Таким образом, пароль, сгенерированный случайным образом имеет большую энтропию, чем пароль, составленный пользователем. В алгоритме работы устройства реализованы функции генерации пароля из допустимых характеристик и максимальной энтропии, хранение пароля на устройстве, улучшение безопасности путем подтверждения действий, считывание пароля из устройства в строку ввода, а также используется защита PIN-кодом.

СПИСОК ЛИТЕРАТУРЫ

1. Васильев, Е. С. Улучшение пользовательский аутентификации с помощью аппаратного менеджера пароля на основе микроконтроллера Arduino / Е. С. Васильев // Проблемы информационной безопасности. – 2017 (18).

2. Домбровская, Л. А. Современные подходы к защите информации, методы, средства и инструменты защиты / Л. А. Домбровская, Н. А. Яковлева, Р. Е. Стахно // Наука, техника и образование. – 2016. – № 4 (22).

3. Лебеденко, А. В. Усовершенствованные способы аутентификации пользователя / А. В. Лебеденко, А. Ю. Мордвинова, Е. С. Васильев // Новая наука: современное состояние и пути ее развития. – Ч. 4. – 2016 (90).

4. Щербаков, А. Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты / А. Ю. Щербаков. – М. : Книжный мир, 2012. – 352 с.

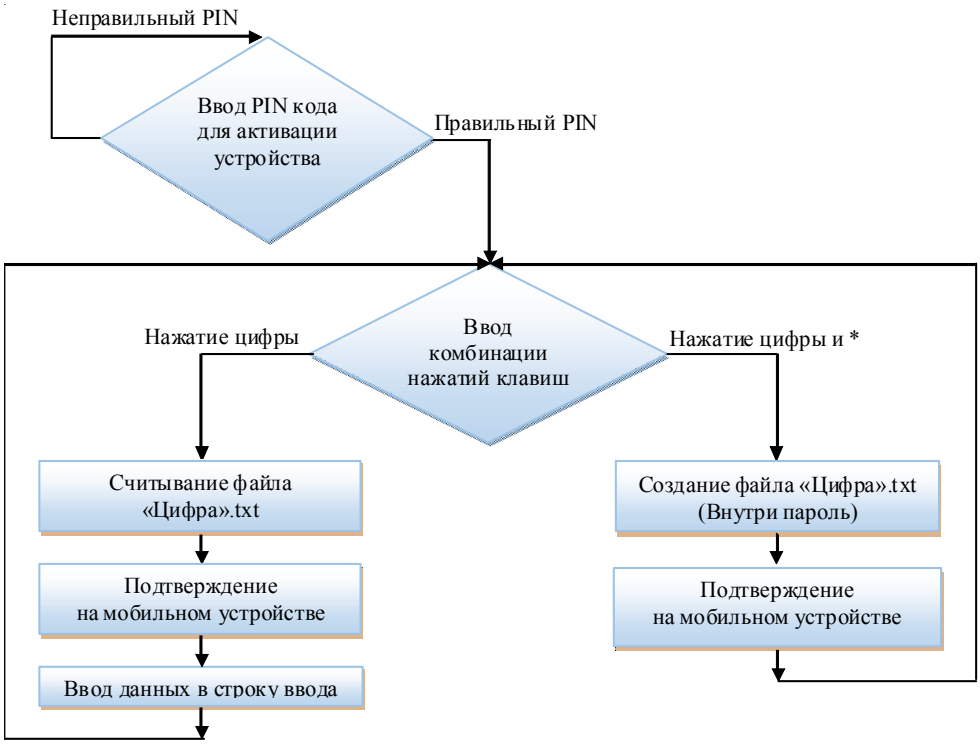

Рисунок. Алгоритм работы устройства

5. Doel, K. Scary Logins : Worst Passwords of 2012 – and How to Fix Them. – Los Gatos : PRWeb, 2012. Electronic text data. – Access mode: https://www.prweb.com/releases/2012/10/prweb10046001.htm. – Screen Title.

6. Sinkov, A. Elementary cryptanalysis: a mathematical approach / A. Sinkov // Mathematical Association of America. – Washington, D.C., 1966. – 222 p.

REFERENCES

1. Vasilyev E.S. Uluchshenie polzovatelskiy autentifikatsii s pomoshchyu apparatnogo menedzhera parolya na osnove mikrokontrollera Arduino [Improving User Authentication with Hardware Password Manager Based on Arduino Microcontroller]. *Problemy informatsionnoy bezopasnosti* [Information Security Problems], 2017, no. 18.

2. Dombrovskaya L.A., Yakovleva N.A., Stakhno R.E. Sovremennye podkhody k zashchite informatsii, metody, sredstva i instrumenty zashchity [Modern Approaches to Information Security, Methods, Means and Tools of Protection]. *Nauka, tekhnika i obrazovanie* [Science, Technology and Education], 2016, no. 4 (22).

3. Lebedenko A.V., Mordvinova A.Yu., Vasilyev E.S. Usovershenstvovannye sposoby autentifikatsii polzovatelya [Advanced User Authentication Methods]. *Novaya nauka: sovremennoe sostoyanie i puti ee razvitiya*, 2016, Part 4, (90).

4. Shcherbakov A.Yu. *Sovremennaya kompyuternaya bezopasnost. Teoreticheskie osnovy. Prakticheskie aspekty* [Modern Computer Security. Theoretical Bases. Practical Aspects]. Moscow, Knizhnyy mir Publ., 2012. 352 p.

5. Kevin D. *Scary Logins: Worst Passwords of 2012 – And How to Fix Them.* Los Gatos, PRWeb, 2012.

6. Sinkov A. Elementary Cryptanalysis: A Mathematical Approach. *Mathematical Association of America*. Washington, D.C., 1966. 222 p.

THE ANALYSIS OF THE PROPERTIES AND CHARACTERISTICS OF PASSWORDS FOR A HARDWARE MANAGER BASED ON ARDUINO MICROCONTROLLER

Alexey V. Lebedenko

Senior Lecturer, Department of Information Security,
Sevastopol State University
avlebedenko@sevsu.ru
Universitetskaya St., 33, 299053 Sevastopol, Russian Federation

Evgeny S. Vasilyev

Student, Department of Information Security,
Sevastopol State University
1996vasilyev@gmail.com
Universitetskaya St., 33, 299053 Sevastopol, Russian Federation

Abstract. The use of passwords is one of the most popular ways to authenticate users on the Internet. Because of the specificity of storing passwords, developers are forced to impose restrictions on which passwords are safer to use. For example, most often a password must contain at least 8 characters, have letters of different registers, contain special characters, etc.It can be stated that over time, these restrictions only increase, and this in turn complicates the choice of a secure and at the same time easy-to-remember password. For example, the most secure password will contain 128 characters with maximum entropy.

The article is devoted to user authentication, password entropy and valid passwords for websites, methods for improving authentication by developing a hardware password manager based on Arduino microcontroller.

Thus, a password generated randomly has more entropy than a password generated by the user. The algorithm of the device includes functions of generating a password from the permissible characteristics and maximum entropy, storing the password on the device, improving security by confirming actions, reading the password from the device to the input line, and using the pin-code protection.

Key words: password entropy, valid password values, device operation algorithm, password characteristics, microcontroller.