THE PROBLEM OF PASSWORD VULNERABILITY IN OUR TIME

Бирилло А. А.

Belarusian State University of Informatics and Radioelectronics
Minsk, Belarus

Перевышко А. И. – преподаватель кафедры ин.яз. № 1

This article is devoted to the review of modern passwords in various information systems. The important role of passwords in the everyday life of any person, in protecting confidential information and creating a sense of security is emphasized. This article shows the factors that weaken passwords. Much attention is given to the importance of this investigation development for increasing information security.

A computer information system is a system composed of people and computers that processes or interprets information. Access to the information system is provided by entering a username and password. A password is a word or string of characters used for user authentication to prove identity and access to a resource, which is to be kept secret from others. Currently, passwords don't represent something new for us. From banking and shopping, to games and music, we keep our data safe with a string of digits, letters and symbols. Passwords have been used in computers since their first days. For example, MIT's CTSS, which appeared in 1961, was one of the first open systems using a password. Thanks to the Internet, it was possible to access information systems remotely. It became a true gift for hackers [1].

The research was conducted using an anonymous online survey, personal experience and using statistics from the Internet like bases of compromised passwords [2]. The main password cracking methods were also considered, such as brute force, wordlist attacks, rainbow table attacks [3]. For example, to assess the effectiveness of brute force was used John the ripper with default order of cracking modes [4-5]. Available passwords were evaluated according to certain criteria: character type exclusivity, length, prevalence of password in dictionaries, rainbow table risk [6]. Of all these properties, length is the most valuable, although it is not an unconditional guarantee of safety.

The results of the analysis showed that in any information system there is a sufficiently large amount of vulnerable passwords. It is annoying that people don't understand the importance of their passwords. For example, more than half of all passwords can be easily cracked using rainbow tables. Truly unique passwords are rare today. Moreover, often the same password is used on different resources. It also increases the possibility of hacking.

Many people are too lazy to memorize complex passwords. Unfortunately, young people also do not think about the security of their passwords using publicly available information to create them. An attack on such digital keys would succeed. Passwords such as "1998АНЯ" and "winner" have been detected. Not surprisingly, the older generation also uses vulnerable passwords more often. These facts show the necessity to work with all information system users. A large number of respondents believe that they are not threatened hacking and that they do not have important information on the net. Furthermore, if you compile your own vocabulary, focused on a specific person, the probability of hacking is greatly simplified. Of course, two-step authentication almost completely eliminates the possibility of hacking, but at present it is not everywhere and not everyone has the opportunity to use it.

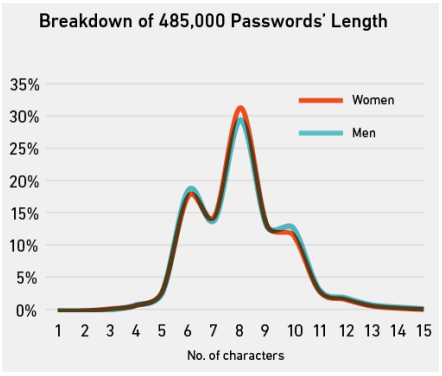
Findings: there are currently too many weak passwords. The battle to secure user passwords will continue as computing power grows. However, work to improve security should not be done only from users. On the server side, proper salt hashing should be applied. Users should be informed about the need to use strong passwords. It is necessary to limit the use of weak passwords in the system and force users to change them. Encourage users to use special software to store passwords in encrypted form. Do not allow the use of the common passwords in different systems. The user must restrict access to personal information by unauthorized persons. Users are strongly advised to follow the following rules when working with passwords:

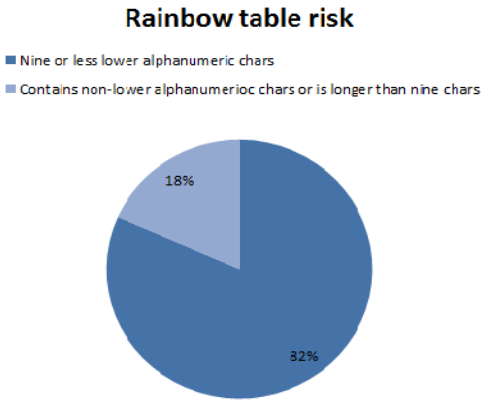
1) passwords should be changed regularly;
2) don't re-use passwords across sites;
3) don't write down your passwords near the computer;
4) avoid phishing(Don't follow unfamiliar links from suspicious individuals or mail);
5) never tell answers to security questions for your mail;
6) use two-step authentication wherever it possible;
7) do not allow the browser to save your passwords;
8) use comprehensive security software and install security patches;
9) avoid entering passwords when using unsecured Wi-Fi connections (like at the airport or coffee shop).

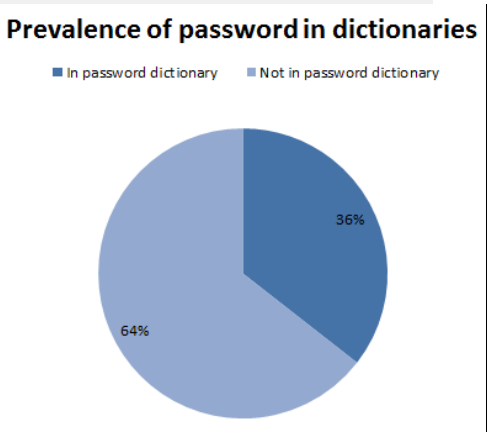
The user must follow the tertian rules when creating a password:

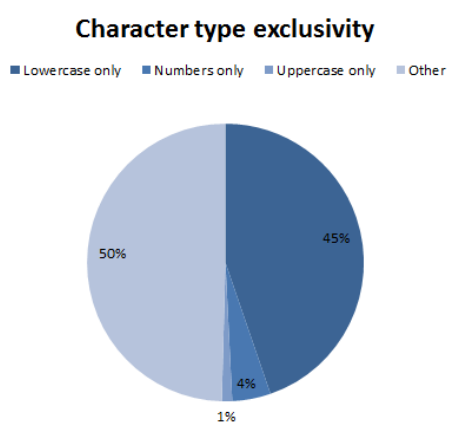
1) don't use personally identifiable information;

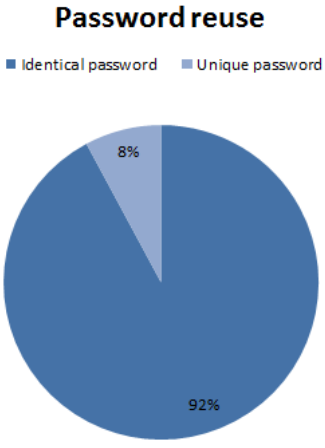
2) avoid common dictionary words;
3) make sure that at least ten or twelve characters are used.;
4) include numbers, symbols, and both uppercase and lowercase letter;
5) don't use a password that matches the site URL or domain name and application name;
6) never use a password that matches the e-mail or username;
7) random passwords are the strongest. If you're having trouble creating one, you can use a password generator instead.











Examples of real passwords used by my peers:

:1999ТАНЯ:
:32violino:
:RammsteinLindemann8870:
:ifahiz94:

References:

1. Herbert Bos, Andrew S. Tanenbaum "Modern Operating Systems" (4th Edition);
2. Pwned Paswords [Электронный ресурс] . – Режим доступа: https://haveibeenpwned.com/Passwords . – Дата доступа: 6.03.2019
3. George Khalil "Password Security--Thirty-Five Years Later";
4. John the Ripper usage examples [Электронный ресурс] . – Режим доступа: https://www.openwall.com/john/doc/EXAMPLES.shtml . – Дата доступа: 9.03.2019;
5. Kali Linux - Password Cracking Tools [Электронный ресурс] . – Режим доступа: (https://www.tutorialspoint.com/kali_linux/kali_linux_password_cracking_tools.htm) . – Дата доступа: 12.03.2019;
6. How Rainbow Tables work [Электронный ресурс] . – Режим доступа: http://kestas.kuliukas.com/RainbowTables . – Дата доступа: 4.03.2019;