UDC 044.92:004.05

PROCEDURES ANALYSIS FOR EVALUATING RESISTANCE OF PASSWORDS

Stud. M. S. Marenych, gr. BIT-17
Language and scientific supervisor S.O. Krasniuk
Kyiv National University of Technologies and Design

It's not a secret to anyone that most of the user authentication systems use password protection today. This applies to personal computers, corporate computers, web applications, ssh / pgp keys. A password is a set of characters intended to confirm the identity of the system user. Passwords are used to protect information from illegal access. For users it is one of the most convenient options, which does not require special knowledge. From the point of view of information security, such authentication cannot be considered completely safety. There are two problems: human factor and technical backwardness. Most users do not want or cannot remember complicated passwords and do not realize how easy it is to crack their password. Therefore, it is necessary to check the password stability to cracking at the stage of its creation by the user and prohibit the entry of weak combinations.

The purpose of this work is to analyze and develop an efficient estimator the password stability to cracking.

To achieve this goal, the following tasks were set and solved:

- Analysis of methods of hacker attacks on password systems.
- The study of data on unstable to cracking passwords.
- Algorithm design for assessing the stability of passwords based on all the analyzed data.

The subject and object of the study are methods of hacker attacks on password systems, data on unstable to cracking passwords, algorithm for assessing the stability of passwords.

Methods and means the study collect general information on this topic. Many scientists have been researching in this area before. The Andersen formula was derived to quantitative assessment stability of passwords. The research was also conducted by Meshcheryakov R.V. and he developed the method of assessment password spaces depending on the alphabet for passwords. [4].

The scientific novelty and practical importance are that password system cracking is a very common hacker attack. In case of success of such an attack, the attacker gets full access to the functions and data of the system, which determines the popularity of this method and the importance of researching methods of protection against it.

Research results For the study data from 967 passwords from one of the cracked mail servers of the Internet was taken. A password of a small number (up to 5) characters / digits is definitely weak. 335 passwords (almost a third) consisted solely of numbers. Only 2 passwords contained special characters. In 33 cases, the user name and password coincided. The most popular was the password 123 (met 35 times, almost every 27 password). The second place is the qwerty password (20 passwords). Then follow: 777 (18 times), 12 (17 times), hacker (14 times) and 1, 11111111, 9128 (10 times). 16 passwords consisted of one character / number.

Algorithm for assessing the stability of passwords

So, based on the analyzed data of possible ways of hacking attacks also on the basis of researched data about deliberately weak passwords, we obtain the following algorithm:

1. At the entrance we get a password for analysis.
2. Account entropy with help of:

- brute force algorithm (full search of all possible combinations of all possible characters);
- dictionary testing algorithm (dictionaries of different languages, film titles, names);

• verification of repetitive passwords (repeating of the same characters, numbers, words);

• checking alphabetic and numerical sequences (for example, 12345, qwerty, abcdef);

• regular expression check (number of characters in the upper and lower case, numbers, and special characters);

• checking dates and years (often in passwords use a year of birth, dates of holidays, and prominent passwords).

Calculate the minimum amount of time needed to crack the given password.

The main result of the algorithm is the password entropy. In order to calculate the cracking time, you need to set the following configuration options:

• T - Password system response time to one request.

• N - Number of cores used by hackers.

Creaking password time is calculated according to the following formula [5]:

$t = 2(E-1)\cdot T$

where :

E - password entropy,

T - is the time for choosing a password.

Conclusions As a result of this work, the tasks were accomplished:

• analyzed modern methods of hacker attacks on password systems,

• data on unstable to cracking passwords was studied,

• based on this, analgorithm for assessing the stability of passwords has been designed.

This algorithm can be used to check the password at the stage of its creation by the user and to prohibit the introduction of weak combinations. The algorithm can be configured for the needs of different systems.

Key words: hacker attacks on password systems, passwords, Andersen formula, methods of protection, algorithm for assessing the stability of passwords, check the password.

REFERENCES:

1. Жуков И.Ю., Иванов М.А., Осмоловский С.А. Принципы построения криптостойких генераторов псевдо случайных кодов // Проблемы информационной безопасности. Компьютерны есистемы. 2001, №1.

2. Зензин О.С., Иванов М.А. Стандарт криптографической защиты - AES. Конечные поля. Серия СКБ (специалисту по компьютерной безопасности). Книга 1.М.: КУДИЦ-ОБРАЗ, 2002.

3. Немнюгин С.А. Программирование - СПб.: Питер, 2000.

4. Мещеряков Р.В. Теоретические основы информационной безопасности автоматизированных систем / Мещеряков Р.В., Праскурин Г.А. – Томск: Из-во Томск. межвуз.центрдист. образ., 2005. – 243 с.

5. Fluhrer S.R. Statistical analysis of the alleged RC4 keystream generator / S.R. Fluhrer, D.A. McGrew // Fast Software Encryption, Cambridge Security Workshop Proceedings. - 2000.