Relationship between security and usability – authentication case study

Miloslav Hub, Jan Čapek, Renáta Myšková

***Abstract*—**In this paper there is discussed relation between seemingly independent aspects of software quality – security and usability. This relation is demonstrated in case study of password authentication. For this purposes a method of password security is suggested and described in this paper. This method consists in mathematical model of dictionary attack and brute force attack. This model is used to break passwords gained from two studies. In these two studies different groups of end users were instructed to select a password by a different way. Afterwards, in security of selected passwords was examined and compared with their usability and this relationship were examined.

***Keywords*—**Authentication, brute force attack, data security, dictionary attack, passwords, usability

I. Introduction

DATA security is an actual issue that is being discussed, especially in the public administration domain and solving spatially oriented problems [1], [2], [3] for the value of information that data contain [4], [5]. One of requirements on secure information systems is a secure authentication of persons working with these systems. Although many mature authentication mechanisms exist (for example smart cards, biometrics), currently passwords are still used for these purposes [6], [7], [8]. The reasons of passwords using are low expenses and easiness of implementation.

Although this way of authentication is generally accepted by end users, passwords have many of the deficiencies arising from limitation of human memory [9]. It is difficult for end users to remember long strings that contain randomly generated characters. That is why the end users select as their passwords commonly used words like names of football clubs, names of pets and so on. Sure, these weak passwords are not resistant against a dictionary attack and a brute force attack. In the recent literature there exists an evidence of weakness of real used passwords against these types of attack [10], [11].

When forcing the users to create strong passwords (it means passwords that are long enough, randomly generated and used only to one system), the users write them down or forget them [12]. This user behavior can make social engineering attack easier.

That is why the passwords authentication appears to involve a tradeoff. It seems more secure password means the less usable password.

Generally, usability of user interface is the extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use. Usability is one of quality aspects of software and consists of the following criteria: learnability, efficiency, memorability, errors and satisfaction [13] and can be examined in different types of user interface, from commercial web pages to e-learning systems [14].

II. Problem formulation

As mentioned above, passwords authentication appears to involve a tradeoff between security and usability. A lot of authors frequently discuss about the factors that influence password security, for example: length, randomness, and the period the password is used. Some authors are trying to make a distinction between a “weak” and a “strong” password, commonly by using an expert’s opinion [12]. Other authors are trying to break passwords, and the results of their experiments are present as a proof of the passwords weakness [11], [15].

The authors of this paper are convinced about the need for investigation of an influence of security and usability. As a case study the authors decided to investigate just a passwords authentication. Next, authors feel necessity of more exact evaluation of the security of passwords.

For this reasons the authors are suggesting the exact measure of security of given password and conducting surveys and experiments with the goal to compare different security level passwords with their usability.

III. Security of given password

A. General Principle

There are various factors that influence a password authentication security. As it is depicted on fig. 1, that is modified on the base of [16], it is possible to divide these factors into two basic groups. The first group is formed by human factors and the second group by technological factors.

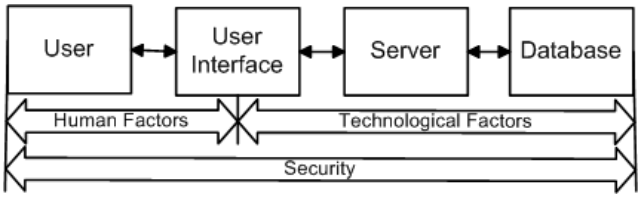

Fig. 1 factors of password authentication security

Human factors that influence can be divided to two categories:

- Type of password (length, randomness, used characters, etc.)
- Mode the user guards a password (how often a user change his password, whether the user writes a password down, and so on)

Since users are thought to be the weakest link of every security solution, it is necessary to study their behavior. We are convinced of the need to study how users choose their passwords, because it evidently infers of security of this kind of authentication.

Because we are interested in passwords type and not technological factors, as a measure of security of a given password we suggest the expected value of the number of attempts an attacker has to carry out to break the password [17]. The advantage of this criterion is non-dependence on technology factors. Time and cost criteria can be derived from this genuine criterion if needed. For example, it is not difficult to determine how many attempts you are required to make per hour in order to successfully crack a password, at a network level.

The evaluation of passwords from a security point of view is composed of two phases:

1) Attack simulation model
2) Password security evaluation, on the base of attack simulation model

B. Attack Simulation Model

When constructing a model of dictionary attack and a brute force attack we formulate two assumptions:

1) Attackers are choosing the most effective way of attack.
2) Attackers know the types of passwords users are selecting.

For simplicity but without losing accuracy, we can think a brute force attack is like a special kind of a dictionary attack. The size of this virtual dictionary can be calculated by eq. (1).

$$N_{VD}(NPC, L) = NPC^{L} \qquad (1)$$

Where:

N_{VD}…The size of a virtual dictionary.
NPC….The number of possible characters.
L……..The length of a password.

Now we can consider a dictionary attack and a brute force attack to be a well-considered sequence of tests performed when trying to know whether a password is a word from a given dictionary. The question is "What dictionary does an attacker use?" on the first attempt, the second, and so on. Based on the assumptions previously discussed, the attacker prefers dictionaries that maximize the probability of his success and minimize the number of attempts to break the password. This criterion can by expressed by eq. (2).

$$SDA(d) = \frac{NBP_d}{N_d \cdot NP} \qquad (2)$$

Where:

SDA(d) Success rate of the dictionary attack on dictionary d.
NBP_d ... The number of passwords that would be broken by dictionary d.
N_d ..... The size of dictionary d.
NP..... Total number of tested passwords used in the attack simulation.

Because we expect the attacker will not test words he has already tested, when sorting dictionaries we recursively remove the used words and reassess unused dictionaries. The overall process is described by the following algorithm.

Step 1: Gather passwords that were used in a given environment by a given kind of users.

Step 2: Gather all possible dictionaries that can contain passwords gathered in step 1. These dictionaries will be used for dictionary attack simulations.

Step 3: Create virtual dictionaries that consists of all one-character strings, two-character strings, and so on, and that can contain passwords gathered in step 1. The sizes of these dictionaries N_{VD} can be calculated by Eq. 1. These dictionaries will be used for brute force attack simulations.

Step 4: Calculate the success rate of the dictionary attack for every dictionary SDA(d), using Eq. 2.

Step 5: If the success rate of the dictionary attack SDA(d) for every dictionary is zero, stop this algorithm, otherwise continue.

Step 6: Select dictionary with maximum attack success rate. This dictionary will be used in the attack simulation model in the order this dictionary was selected.

Step 7: Delete all the words that the selected dictionary contains from the remaining dictionaries. A new set is created for the remaining reduced dictionaries.

Step 8: Repeat step 4 for the set of remaining reduced dictionaries.

C. Password Security Evaluation

The result of previous algorithm is a sorted set of reduced dictionaries that the attacker can use in the event he wants to break a password in the most effective way. Now, it is easy

to calculate the security of a password, which is defined as the expected value of number of attempts the impostor has to carry out to break a password, with help of Eq. 3.

$$S(p_i) = \frac{N_i + 1}{2} + \sum_{j=1}^{i-1} N_j \qquad (3)$$

Where:

$S(p_i)$ .....Security of a password p that is a word from i-th reduced dictionary.

i .....The order of the reduced dictionary that contains a password p.

N_i .....The size of the i-th reduced dictionary.

D. Ordered list of reduced dictionaries

In 2008 we collected 1,895 passwords that were really used on web pages. All users who were selecting passwords were Czech speaking. Passwords had to contain a minimum of one character and maximum length of the password was not restricted. Users had no time limit when selecting a password and passwords could contain arbitrary characters typed using a keyboard.

Firstly, Exploratory Data Analysis (EDA) was applied to the first password collection. The goal of this analysis was to create the basic assumptions about users' behavior, and for pertinent dictionaries selection. Diacritic characters were rarely used in passwords, only in 1.8% passwords. Further, only 10.6 % of passwords contained an uppercase character and 23.2 % of passwords contained a minimum of one numeral.

Users did not use a long string passwords, the length of passwords was about 6 characters (see fig. 2).

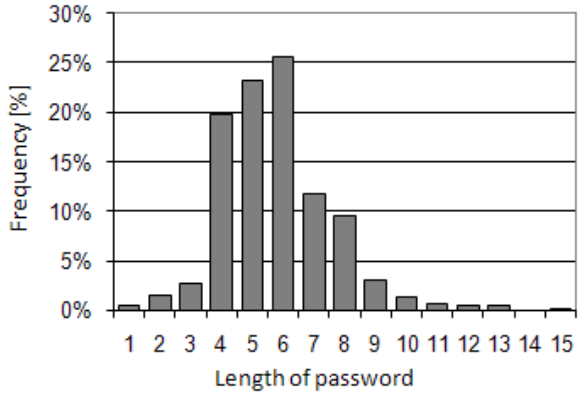

Fig. 2 length of selected passwords

After dividing the acquired passwords into four groups, in relation to the "randomness" of the password, it is possible to see that users prefer common words as their passwords, as you can see in fig. 3.

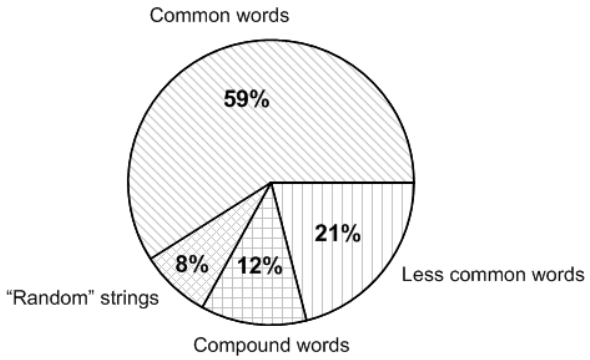

Fig. 3 "randomness" of selected passwords

This assumption is proven when you test the correlation coefficients hypothesis between the frequencies of characters in passwords and the frequencies of characters in Czech words (Kendall rank correlation coefficient equals 0.78) – see table 1.

TABLE I
FREQUENCY OF CHARACTERS

Character	Freqiency in Czech	Frequency in passwords
A	0.086	0.158
B	0.017	0.024
C	0.033	0.027
D	0.036	0.041
E	0.105	0.082
F	0.002	0.009
G	0.002	0.011
H	0.022	0.020
I	0.075	0.065
J	0.022	0.022
K	0.036	0.064
L	0.042	0.051
M	0.035	0.039
N	0.068	0.062
O	0.080	0.070
P	0.032	0.026
Q	0.000	0.001
R	0.049	0.065
S	0.063	0.044
T	0.051	0.047
U	0.040	0.028
V	0.043	0.020
W	0.000	0.007
X	0.001	0.005
Y	0.028	0.006
Z	0.032	0.008

TABLE II
CORRELATION OF CHARACTERS

	Kendall Tau	p-value
Passwords & Czech	0.78	0.000000
Passwords & English	0.62	0.000008

After Exploratory Data Analysis we gathered potential 35 dictionaries that could contain passwords we collected in this research study. We used the algorithm discussed above and created the ordered list of reduced dictionaries. The final order of these reduced dictionaries is as follows:

1) Czech First Names (490 words)
2) Common Czech Words (382 words)
3) Common Passwords (239 words)
4) Czech First Names (the first character uppercase) (490 words)
5) Years 1900 – 2029 (114 words)
6) Common Logins (2,131 words)
7) The Most Commonly Used English Words (391 words)
8) Czech and American Word Combinations (496 words)
9) Word Personages (437 words)
10) American Women Names (4,414 words)
11) American Men Names (3,020 words)
12) Slovak Dictionary (17,952 words)
13) Common Word Connection (796 words)
14) Electronic Firms (41,053 words)
15) Foreign First Names (8,801 words)
16) Czech Dictionary (157,228 words)
17) Bible Characters (10,654 words)
18) Unusual First Names (4,612 words)
19) English Dictionary (317,410 words)
20) States and Towns (68,729 words)
21) Big English Dictionary (581,000 words)

The next 15 complementary dictionaries were formed by virtual dictionaries that simulated a brute force attack that followed a simulated dictionary attack. There is a list of this virtual dictionaries:

22) 1-character words dictionary (36 words)
23) 2-character words dictionary (1,296 words)
24) 3-character words dictionary (46,656 words)
25) 4-character words dictionary (1,679,616 words)
26) 5-character words dictionary (60,466,176 words)
27) 6-character words dictionary (2,176,782,336 words)
28) 7-character words dictionary (78,364,164,096 words)
29) 8-character words dictionary (2,82111E+12 words)
30) 9-character words dictionary (1,0156E+14 words)
31) 10-character words dictionary (3,65616E+15 words)
32) 11-character words dictionary (1,31622E+17 words)
33) 12-character words dictionary (4,73838E+18 words)
34) 13-character words dictionary (1,70582E+20 words)
35) 14-character words dictionary (6,14094E+21 words)
36) 15-character words dictionary (2,21074E+23 words)

The security of passwords from these 36 reduced dictionaries is possible to see in table 3.

TABLE III
SECURITY OF DICTIONARIES

Type of an attack	No. of reduced dictionary	Security of a password	Type of an attack	No. of reduced dictionary	Security of a password
Dictionary	1	245	Dictionary	19	412401
	2	681		20	605471
	3	991,5		21	930335
	4	1354	Brute force	22	1220853
	5	1654		23	1221519
	6	2777		24	1245495
	7	4038		25	2108631
	8	4481		26	3.32E+7
	9	4948		27	1.15E+9
	10	7373		28	4.14E+10
	11	11090		29	1.49E+12
	12	21576		30	5.37E+13
	13	30950		31	1.93E+15
	14	51875		32	6.96E+16
	15	76802		33	2.50E+18
	16	159816		34	9.02E+19
	17	243757		35	3.25E+21
	18	251390		36	1.17E+23

IV. EXPERIMENTAL STUDY 1

In 2009 we conducted an experiment inspired by [18] in which we asked 64 students to choose passwords and write them to questionnaires. These questionnaires also assigned a random password to each student. The random password had from 6 to 7 characters.

Next, students were trained how to create a passphrase - a password based on a mnemonic phrase. After this training the students were asked to choose passphrase and write this passphrase down to the questionnaire.

By this way three passwords were assigned to every student – a common password, a randomly generated 6-7 characters

long password and a passphrase. The students were asked to remember all passwords and do not write them down. Two months later this participants were requested to recall these three passwords and write them down to prepared forms. We found the following results (see table 4):

TABLE IV
RECALL OF DIFFERENT PASSWORD TYPES

	Self-selected	Passphrase	Random
Sucessful recall	45%	34%	12%
Unsucessful recall	55%	66%	88%

However, the participants were not actually using the password during the intervening two months. But the results of this experiment provide a quantitative point of reference for the difficulty of random passwords. From this table (table 2) it is possible to see that self-selected passwords and passphrase passwords have similar results and passphrase passwords are easy to remember like self selected passwords.

In the next phase of this experiment we put acquired passwords to the simulated dictionary attack and brute force attack and evaluated them from the security point of view. The goal was to compare the security of passwords created by different methods. The results of these simulated attacks are shown in the table 5.

TABLE V
SECURITY OF DIFFERENT PASSWORDS TYPES

Type of an attack	No. of reduced dictionary	Security of a password	Self-selected passwords	Passphrase passwords	Random passwords
Dictionary	1	245	7	0	0
	2	681	3	0	0
	3	992	1	0	0
	4	1354	1	0	0
	5	1654	0	0	0
	6	2777	2	0	0
	7	4038	0	0	0
	8	4481	0	0	0
	9	4948	0	0	0
	10	7373	3	0	0
	11	11090	0	0	0
	12	21576	1	0	0
	13	30950	0	0	0
	14	51875	2	0	0
	15	76802	3	0	0
	16	159816	2	0	0
	17	243757	0	0	0
	18	251390	0	0	0
	19	412401	1	0	0
	20	605471	0	0	0
	21	930335	4	0	0
Brute force	22	1220853	0	0	0
	23	1221519	1	0	0
	24	1245495	0	0	0
	25	2108631	4	4	0
	26	3.32E+7	4	28	0
	27	1.15E+9	13	24	32
	28	4.14E+10	3	7	32
	29	1.49E+12	3	1	0
	30	5.37E+13	1	0	0
	31	1.93E+15	1	0	0
	32	6.96E+16	0	0	0
	33	2.50E+18	0	0	0
	34	9.02E+19	1	0	0
	35	3.25E+21	0	0	0
	36	1.17E+23	0	0	0

From the results of simulated dictionary attack and brute force attack we can claim, that no random password and no passphrase password is possible to break dictionary attack and these types of passwords have password security more than 1245495. By contrast to these types of passwords, self selected passwords are sensitive against dictionary attack. For example after 930,335 attempts to break self-selected password, this password will be broken by probability about 0.5 (see fig. 4).

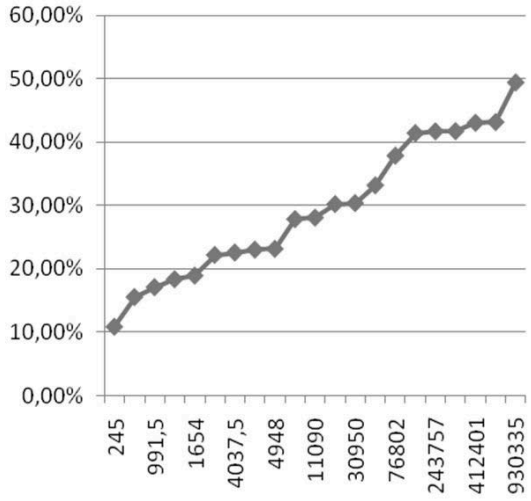

Fig. 4 dictionary attack to self-selected passwords

V. EXPERIMENTAL STUDY 2

This experimental study that was inspired by [18] was conducted in 2010. The goal of this experimental study was to investigate the tradeoff between security and memorability in the real world context. In this experiment 56 two-years students at University of Pardubice were divided to three experiment groups. Afterwards each student was given a sheet of advices how to create a password depending on the group with he has been randomly assigned.

The three different types of advices were:

- Control group. The participants in this group were given the same advice as in previous years, with was simply that "Your password should contain both alphabetical and numerical characters and should be long".
- Random password group. The participants in this group were given a printed sheet with the letters A-Z and numbers 1-9 repeadly on it. They were asked to choose random password by closing their eyes and picking seven character at minimum. The participants were told to write the chosen password down and destroy it once the password was memorized.
- Passphrase group. The participants in this group were asked to choose a password based on a mnemonic phrase.

The number of participants in these three groups was following (see table 6):

TABLE VI
NUMBER OF PARTICIPANTS

	Control group	Random password group	Passphrase group
Number of participants	18	19	19

The participants were using their passwords one times a week at minimum. We conducted this experiment one month. During this period we calculated the numbers of requests of password reset in the situation when a student forgot his password). The exact number of these requests it possible to see in table 7.

As it was expected, maximal requests of password reset came from random password group. The reason is that randomly generated password is difficult to remember.

TABLE VII
NUMBER OF REQUESTS OF PASSWORD RESET

Group	Number of requests
Control group	1
Random password group	4
Passphrase group	2

One month after the tutorial session we asked the students to fill questionnaires, asking whether they'd had difficulty remembering ther password. This survey asked the following questions:

- How hard it was to memorize your password (scale from 1 – trivial to 5 – impossible)?
- How many weeks did you need to remember your password?

The results of this survey are summarized in the table 8. From this table it is possible to see that it is difficult to remember randomly generated password.

TABLE VIII
RESPONSES TO THE MEMORABILITY SURVEY

	Difficulty level (1-5)	Weeks
Control group	2.2	0.2
Random password group	3.8	4.5
Passphrase group	2.6	1.2

At the end of this survey we used gained passwords in model of dictionary attack and brute force attack. As we expected, the results of control group were worse than results both random password group and passphrase group. While it was possible to break 10 passwords from control group by dictionary attack no password was possible to break by this type of attack from password and passphrase groups. The results of these simulated attacks you can see in table 9.

TABLE IX
SECURITY OF DIFFERENT PASSWORDS TYPES

Type of an attack	No. of reduced dictionary	Security of a password	Control group	Random password group	Passphrase group
Dictionary	1	245	0	0	0
	2	681	0	0	0
	3	992	1	0	0
	4	1354	0	0	0
	5	1654	3	0	0
	6	2777	0	0	0
	7	4038	2	0	0
	8	4481	1	0	0
	9	4948	0	0	0
	10	7373	0	0	0
	11	11090	0	0	0
	12	21576	2	0	0
	13	30950	0	0	0
	14	51875	0	0	0
	15	76802	0	0	0
	16	159816	0	0	0
	17	243757	1	0	0
	18	251390	0	0	0
	19	412401	0	0	0
	20	605471	0	0	0
	21	930335	0	0	0
Brute force	22	1220853	0	0	0
	23	1221519	0	0	0
	24	1245495	0	0	0
	25	2108631	0	0	0
	26	3.32E+7	2	0	3
	27	1.15E+9	3	2	5
	28	4.14E+10	1	8	3
	29	1.49E+12	1	6	4
	30	5.37E+13	0	3	2
	31	1.93E+15	1	0	2
	32	6.96E+16	0	0	0
	33	2.50E+18	0	0	0
	34	9.02E+19	0	0	0
	35	3.25E+21	0	0	0
	36	1.17E+23	0	0	0

VI. CONCLUSION

Although security and usability are separate aspects of software quality; there exists dependence between these two aspects. This dependence is proved on authentication by passwords. When forcing end users to use more secure passwords, these passwords are less learnable and memorable.

It is confirmed that users have difficulty to remember random passwords. Only 12 percent of users were able to recall these passwords after two months. But passwords based on mnemonic phrases are more memorable then random passwords and they have the similar security level. By educating users to use mnemonic passwords we can gain a significant improvement in security.

But we assume that there can by different type of dependency between usability and security. In some cases a higher usability can results in higher security, when end users do not do mistakes that can result in security faults. As an example a password written down to a calendar because it is very difficult to remember can be noted.

ACKNOWLEDGMENT

This paper was created with a support of the Grant Agency of the Czech Republic, grant No. 402/08/P202 with the title Usability Testing and Evaluation of Public Administration Information Systems and grant No. 402/09/0219 with title Usability of software tools for support of decision-making during solving spatially oriented problems.

REFERENCES

[1] P. Sedlák, J. Komárková, A. Piverková. Spatial analyses help to find movement barriers for physically impaired people in the city environment - Case study of pardubice, Czech Republic. *WSEAS TRANSACTIONS on INFORMATION SCIENCE & APPLICATIONS*. Greece: WSEAS Press, 2010, Volume 7, Issue 1, s. 122-131, ISSN: 17900832.

[2] P. Sedlák, J. Komárková, A. Piverková. Geoinformation Technologies Help to Identify Movement Barriers for Physically Impaired People. In *Scientific Papers of the University of Pardubice : Series D.* Special Edition. Pardubice: Univerzita Pardubice, 2009. p. 125-133. ISSN 1211-555X. ISBN 978-80-7395-209-9.

[3] P. Sedlák, J. Komárková, M. Jedlička, R. Hlásný, I. Černovská. The use of modelling tools for modelling of spatial analysis to identify high-risk places in barrier-free environment. *INTERNATIONAL JOURNAL OF SYSTEMS APPLICATIONS, ENGINEERING & DEVELOPMENT*, Issue 1, Volume 5, 2011. ISSN 2074-1308.

[4] R. Myšková.Economic dimense of value of information (originally in Czech). *Scientific Papers of the University of Pardubice*, Series D , 2006 , č. 10 , s. 228-232.

[5] J.Valášek, J.: Zranitelnost prvků kritické infrastruktury. In: *Informační zpravodaj*, ročník 17, číslo 1, 2006. MV-GŘ HZS ČR, Institut ochrany obyvatelstva, Lázně Bohdaneč. ISBN 80-86640-60-4.

[6] A. AlAzzazi, A. E. Sheikh, Security Software Engineering: Do it the right way, *Proceedings of the 6th WSEAS Int. Conf. on Software Engineering*, Parallel and Distributed Systems, Corfu Island, Greece, pp. 19-23, 2007.

[7] Y. C. Lee, Y. C. Hsieh and P. S. You, A New Improved Secure Password Authentication Protocol to Resist Guessing Attack in Wireless

Networks, *Proceedings of the 7th WSEAS Int. Conf. on Applied Computer & Applied Computational Science (ACACOS '08)*, Hangzhou, China, pp. 160-163, 2008.

[8] W. G. Shieh, M. T. Wang. An improvement on Lee et al.\'s noncebased authentication scheme . In *WSEAS Transactions on Information Science and Applications*. Vol.1, WSEAS Press, 2007. pp. 832-836. ISSN 1790-0832.

[9] J. Yan, A. Blackwell, R. Anderson, A. Grant, The Memorability and Security of Passwords. *Security and usability*. O'Reilly Media, Inc. 2005. pp 129-142. ISBN 0-956-00827-9.

[10] F. T. Gramp, R. H. Morris. *Unix Operating System Security*. AT and T Bell Laboratories Technical Journal 63:8 (Oct. 1984), 1649-1672.

[11] D. V. Klein. Foiling the Cracker: A Survey of, and Improvements to, Password Security (revised paper*). Proceedings of the USENIX Security Workshop* (1990).

[12] M. Burnett, D. Kleiman. ed. *Perfect Passwords*. Rockland, MA: Syngress Publishing. 2006. p. 181. ISBN 1-59749-041-5.

[13] International Standards Organisation (ISO). *International Standard ISO 9126. Information technology: Software product evaluation: Quality characteristics and guidelines for their use*. 1991.

[14] M. Černá, P. Poulová. User testing of language educational portals. *E+M Economics and Management*, (3) s. 104-117. Liberec 2009. ISSN 1212-3609.

[15] Ch. P. Garrison, An Evaluation of Passwords, *On line CPA Journal*- May 2008, Accesable http://www.nysscpa.org/cpajournal/2008/

[16] K. Renaud, Evaluating Authentication Mechanism. *Security and usability*. O'Reilly Media, Inc. 2005. pp 103-128. ISBN 0-956-00827-9.

[17] M. Hub, J. Čapek. Method of Password Security Evaluation. In GUO, Qingsping, GUO, Yucheng. *The 8th International Symposium on Distributed Computing and Applications to Business, Engineering and Science*. [s.l.] : [s.n.], 2009. s. 401-405. ISBN 978-7-121-09595-5.

[18] M. Zviran, W. J. Haga. A Comparasion of Password Techniques for Multilevel Atuthentication Mechanism. *Computer Journal* 36:3 (1993), 227-237.