Online ISSN 1848-3380, Print ISSN 0005-1144
ATKAFF 56(1), 69–75(2015)

Kresimir Solic, Hrvoje Ocevcic, Damir Blazevic

Survey on Password Quality and Confidentiality

DOI 10.7305/automatika.2015.04.587
UDK [681.518-052:004.056](049.5)

Original scientific paper

In this paper are presented results of empirical survey on password quality self-assessment and several privacy issues regarding password manipulation among information systems' users. Data was collected by questioning 627 e-mail users that were adults, Croatian national and were using e-mail system on regular basis. Comparisons among different kind of users were done regarding age, gender, technical background knowledge, university degree and experience in usage. Results of statistical analysis have shown that most of the users' passwords are of average quality while 13,8% of all users graded their password as poor. Regarding password manipulation 53,4% of all users said they use the same passwords for most of the information systems they use. In total 20,7% of all users sometimes lend their password and 17,1% of them wrote it down for remembering. Results of this study highlighted importance of using security procedures and guidelines and need of the continuous education on security issues with constant informing and alerting of information systems' users. This study is an example on how to evaluate different users' security awareness in order to adjust courses on security issues and to adapt informing and alerting to different groups of information systems' users. However, there is great need for validated universal questionnaire for this kind of surveys.

Key words: Information Security, Password, Privacy, Security Awareness, Human Influence

Anketno istraživanje na temu kvalitete i povjerljivosti zaporke. U ovome radu su prikazani rezultati empirijskog istraživanja koje je provedeno anketiranjem korisnika informacijskih sustava na temu samoprocjene kvalitete zaporke te nekoliko elemenata po pitanju privatnosti i povjerljivosti zaporke. Podaci su prikupljeni anketiranjem 627 korisnika informacijskog sustava elektroničke pošte. Svi su bili punoljetni i Hrvatski državljani koji redovito koriste sustav elektroničke pošte. Korisnici su grupirani u kategorije s obzirom na spol, starosnu dob, tehničko predznanje, stupanj obrazovanja te iskustvo u korištenju sustava kako bi se napravila usporedna analiza. Rezultati su pokazali da većina korisnika procjenjuje svoju zaporku ocjenom *prosječno*, dok 13,8% od ukupnog broja korisnika procjenjuje svoju zaporku ocjenom *loše*. Po pitanju manipulacije zaporkom, 53,4% korisnika je odgovorilo kako preferiraju koristiti istu zaporku za pristup većini korištenih informacijskih sustava; 20,7% korisnika je barem jednom posudilo svoju zaporku; dok je 17,1% korisnika negdje zapisalo svoju zaporku. Rezultati ove studije ističu važnost korištenja sigurnosnih procedura i uputa te potrebu za stalnom edukacijom, informiranjem i alarmiranjem korisnika informacijskih sustava po pitanjima informacijske sigurnosti. Također ova studija može biti primjer kako analizirati pojedine vrste korisnika, a u svrhu prilagođavanja tečajeva na temu informacijske sigurnosti, te osmišljanja metoda informiranja i alarmiranja korisnika. Postoji realna potreba za razvojem univerzalnog upitnika koji bi bio međunarodno validiran te se ne bi zasnivao samo na pitanjima vezanim uz zaporku.

Ključne riječi: informacijska sigurnost, zaporka, privatnost, svijest o sigurnosti, utjecaj čovjeka

1 INTRODUCTION

It is common knowledge that users with their potentially risky behavior, caused by low security awareness, can significantly influence on overall system's security [1]. Also e-mail system is one of the most corrupted communication channels with significant increase of direct phishing attack attempts [2].

Because password is one of the several main information system's security issues the aim of this study is to analyze quality of e-mail users' passwords and their attitude towards its privacy regarding user's age, gender, technical background knowledge (e.g. engineers and system administrators vice economists and medical doctors), university degree and experience in usage.

Starting premise was that users with technical background knowledge and experience in usage will act in more secure manner regarding password usage. Also it was expected not to find significant difference regarding age, gender or university degree among examined users.

In this research e-mail users were considered private or single users and not users of a controlled business information system as its employees.

1.1 About Passwords

Password is a secret word or a string of characters that is used for user authentication to prove identity, or for access approval to gain access to an information resource. Historically, passwords are always exchanged, initially verbally, in order to realize the rights of access to a property or knowledge. In modern times, user names and passwords are commonly used by people during a logging process that controls access to protected computer operating systems, mobile phones, cable TV decoders, automated teller machines (ATMs), etc. A typical computer user has passwords for many purposes: logging into accounts, retrieving e-mail, accessing applications, databases, networks, web sites, etc.

In this paper password was not considered as a key subject for accessing a particular system trough threat-vulnerability analysis, but as object for measuring the impact of user's behavior on the overall information security.

1.2 Importance of a Good Password

Information security rules and good practices describe some of the rules to follow. Many companies are creating policies and/or procedures for user awareness and some of them are using enforcement tools to implement policies. Tips when creating passwords in manner not to use *personal information* and *real words* can be found in many guidelines [3]. There are tools available to help attackers guess user's password [4-5]. With today's computing power, it doesn't take long to try every word in the dictionary and find searched password, so it is best not to use real, grammatically correct, words for passwords [6].

In order to follow information security guidelines, it is recommended to use *complexity and passphrases* in password. It is possible to make password much more secure by mixing different types of characters and trying to remember created password by using various character types, not a whole words from the dictionary but parts or first letters in sentences, or passphrases.

Password management tools can be used to securely store and remember passwords. These tools maintain a list of usernames and passwords in encrypted form. For larger enterprises, Single-Sign−On (SSO) systems can help alleviate these issues, but SSO systems rarely offer complete coverage of all password needs, leaving security gaps. For smaller organizations, SSO systems are generally cost prohibitive. Some examples of various management password tools are KeePass and Apple's iCloud Keychain [7, 8].

Usage of *different passwords* defines different username and password for each system or application. That way if one password gets compromised the others are still safe [9]. *Changing passwords* is one of many enforcement methods. There is often a policy to change password in some period of time with restriction against its re-use. *Stronger passwords enforcement* is the most widely used tool in companies with numerous users.

It is very important to determine boundary between enforcement policy and structure of employees in different departments. A negative result is often a significant increase in user requirements causing forgotten passwords, locked accounts or the like. The enforcement of a password policy in order to increase password strength and security, considers also some of the following methods:

1. Requiring periodic password changes,
2. Assigning randomly chosen passwords,
3. Requiring minimum password lengths,
4. Prohibition of reusing same password,
5. Various character classes in a password (password complexity),
6. Providing an alternative to keyboard entry (e.g. spoken password or biometric characteristics),
7. Requiring more than one authentication system (such as 2-factor authentication).

1.3 Threats and Weaknesses

There are several ways to attack passwords. The simplest way is also the most effective. If one wants to know someone's password, he/she should use *social engineering methods*. In a study from 2010, through a simulation of what a real social engineer might try to do, researchers were able to get useful demographic and tactical information from the majority of the "victims", with 73% of respondents that shared their password with the researchers [10].

Another way to attack passwords is to capture the challenge-response pairs and then attempt to *crack* those [11]. Crack is a generic term that basically encompasses many different attempting methods in order to guess the password. Cracking the NTLM, in Windows case, challenge response might actually be faster, depending on the character set used and the length of the password. The NTLM challenge-response only three DES computations and one MD4 hash. Computing an MD4 hash is much faster than computing a DES encryption. Different approaches of cracking speeds up cracking time by several orders of magnitude. With development of information technology and awareness there is also development of encryption algorithms that greatly help in increasing the security of information assets protected by passwords.

Another way to attack passwords is to break into the part of information system that stores the *hashes*, for example domain server or web server. Those hashes could then be cracked using essentially the same technique as for captured challenge-response pairs, but using far fewer computations.

Also key-loggers or other different devices are used in order to record input strings by the user, often as malicious programs for personal computers.

2 MATERIALS AND METHODS

Questionnaire regarding security of e-mail usage was used including questions regarding password quality and its confidentiality. In one question users were asked to grade their password's quality; in another they were asked if they use the same or prefer different passwords for different systems; in next questions they were asked if they wrote down their password somewhere in case of forgetting it and if they ever lend their password to some "friend in need". Detailed explanation of used questionnaire can be found in previously published paper [12].

In first question, in order to self-assess their password, examinees got short explanation written in brackets next to the question, what was meant as *good* and what was meant as *poor* password quality. Grade *good* means that password is combination of small letters, capital letters and numbers, but not a dictionary word, and that is at least eight characters long. Grade *poor* means that password is some kind of a name, meaningful word or number and/or that is shorter than six characters. That way grade *average* of password quality was between those two defined grades.

Categorization of users was done regarding different demographic variables as listed below:

1. Differentiation regarding gender,
2. In categorization regarding age, users were divided into two groups with margin defined at 21 years of age,
3. Users were differentiated regarding possible possession of technical background knowledge depending on their working experience and/or kind of education (technical or not),
4. Users were defined into two groups regarding university degree as with or without degree.
5. Differentiation into two groups regarding experience in e-mail usage was done dependent on total number of e-mail addresses used (one address vice more addresses used).

Data was collected by questioning 627 e-mail users that were adults, Croatian nationality and were using e-mail system on regular basis. Statistical analysis was conducted by STATISTICA 10.0 software tool, while level of significance was defined as p<0,05. All collected data were categorical and Chi-square test was used for correlation testing.

3 RESULTS ANALYSIS

Main results are shown in figures below. Regarding self-assessment of password quality 86 e-mail users out of 627 of all examinees grade their password as *poor*, 296 of all users grade their password as *average* and 243 of users grade their password as *good* quality (Fig.1).

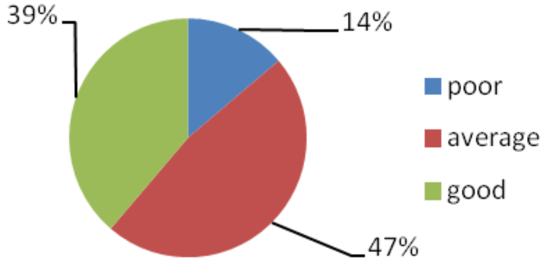

Fig. 1. Grade proportions of password quality self-assessment among users

Most users are reusing the same password for several different systems (53,4%) while around 20% of all users has written down their password (17,1%) and/or lend their password to somebody else (20,6%) (Fig.2).

Comparing results regarding age, gender, technical background knowledge, university degree and experience in usage are shown in tables below.

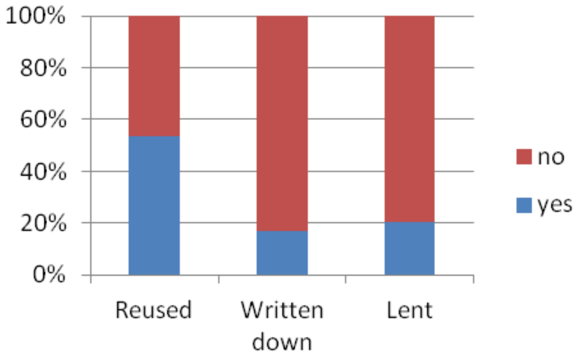

Fig. 2. Proportions of password privacy handling/manipulation

Comparing password quality self-assessment statistically significant difference was not found only when differentiating users regarding university degree as both groups of users had similar distribution of grades. Analysis on other user differentiations has shown that young users, male users, users with technical background knowledge and more experienced users have significantly better password quality (Table 1).

Table 1. Distribution of password quality self-assessments

	Password Quality Grades				
	Poor	***Average***	***Good***	***Total***	***p****
Regarding Age					
<=21	8 (2,5)	174 (55,2)	133 (42,3)	315 (100,0)	<**0,001**
>21	78 (25,2)	122 (39,5)	109 (35,3)	309 (100,0)	
Regarding Gender					
Male	37 (11,4)	139 (42,8)	149 (45,8)	325 (100,0)	**0,001**
Female	49 (16,4)	157 (52,5)	93 (31,1)	299 (100,0)	
Regarding technical background knowledge					
With	16 (11,1)	64 (44,1)	65 (44,8)	145 (100,0)	**0,013**
Without	35 (19,3)	91 (50,3)	55 (30,4)	181 (100,0)	
Regarding university degree					
With	24 (12,0)	99 (49,5)	77 (38,5)	200 (100,0)	0,622
Without	62 (14,6)	197 (46,5)	165 (38,9)	424 (100,0)	
Regarding experience in e-mail usage					
Only one address	39 (19,8)	110 (55,8)	48 (24,4)	197 (100,0)	<**0,001**
More addresses	45 (10,6)	186 (43,9)	193 (45,5)	424 (100,0)	

*Chi-square Test

Results of the analysis have shown that young users, users with technical background knowledge and more experienced users significantly more often have same passwords for most of the used, different systems (Table 2).

Analysis on users writing down their password, had found significant differences regarding age, gender and university degree. Older users, female users and users with university degree had significantly oftener written down their password (Table 3).

Comparison on what kind of users has lent their password, has shown that older users and user without university degree has significantly oftener lent their password (Table 4).

Table 2. Distribution of answers on having same password for most of the used systems

	One or More Passwords			
	Yes	***No***	***Total***	***p****
Regarding Age				
<=21	180 (56,8)	137 (43,2)	317 (100,0)	<**0,001**
>21	112 (36,2)	197 (63,8)	309 (100,0)	
Regarding Gender				
Male	155 (47,8)	169 (52,2)	324 (100,0)	0,535
Female	137 (45,4)	165 (54,6)	302 (100,0)	
Regarding technical background knowledge				
With	80 (54,8)	66 (45,2)	146 (100,0)	**0,007**
Without	72 (39,8)	109 (60,2)	181 (100,0)	
Regarding university degree				
With	99 (49,5)	101 (50,5)	200 (100,0)	0,327
Without	193 (45,3)	233 (54,7)	426 (100,0)	
Regarding experience in e-mail usage				
Only one address	79 (40,3)	117 (59,7)	196 (100,0)	**0,034**
More addresses	211 (49,4)	216 (50,6)	427 (100,0)	

*Chi-square Test

Results of empirical analysis have shown that most of the users' passwords are of average quality regarding self-assessment (Fig.1). Regarding password manipulation little less than half users said they use different passwords for most systems they use.

4 DISCUSSION

Weak passwords are still common information security issue. The user - chosen passwords are predictable and can be guessed by using tools such as dictionaries or probabilistic models, but existing literature does not provide an answer to the question on: given a number of guesses, what is the probability that a very good attacker will be able to break a password [13]?

Significant percentage of users chooses easily-guessed text password, the average password length is less than 7 characters and most passwords contain only letters and

Table 3. Distribution of answers on writing down passwords

	Password Written Down			
	Yes	***No***	***Total***	***p****
Regarding Age				
<=21	17 (5,3)	301 (94,7)	318 (100,0)	<**0,001**
>21	91 (29,4)	218 (70,6)	309 (100,0)	
Regarding Gender				
Male	42 (12,9)	283 (87,1)	325 (100,0)	**0,003**
Female	66 (21,9)	236 (78,1)	302 (100,0)	
Regarding technical background knowledge				
With	27 (18,5)	119 (81,5)	146 (100,0)	0,510
Without	39 (21,4)	143 (78,6)	182 (100,0)	
Regarding university degree				
With	46 (22,9)	155 (77,1)	201 (100,0)	**0,010**
Without	62 (14,6)	364 (85,4)	426 (100,0)	
Regarding experience in e-mail usage				
Only one address	36 (18,3)	161 (81,7)	197 (100,0)	0,612
More addresses	71 (16,6)	356 (83,4)	427 (100,0)	

*Chi-square Test

numbers while passwords with special characters are much harder to guess [14].

As passwords are the first line of defense for many computerized systems, quality of these passwords implies on the security strength of these systems. A good quality evaluation tool to prescribe the characteristics of good quality passwords is necessary [15].

As there is insufficient research defining metrics to characterize password strength and using them to evaluate password-composition policies, well defined distributed method for calculating is needed [16].

Also, huge problem is credulity among information system's users. More than two thirds of users would give away their password to the hackers that use social engineering methods [10]. Solution is to develop positive distrust in user's awareness regarding security issues [17].

Table 4. Distribution of answers on lending passwords

	Password Lent			
	Yes	***No***	***Total***	***p****
Regarding Age				
<=21	17 (5,4)	298 (94,6)	315 (100,0)	<**0,001**
>21	112 (36,2)	197 (63,8)	309 (100,0)	
Regarding Gender				
Male	64 (19,8)	260 (80,2)	324 (100,0)	0,555
Female	65 (21,7)	235 (78,3)	300 (100,0)	
Regarding technical background knowledge				
With	23 (15,9)	122 (84,1)	145 (100,0)	0,402
Without	35 (19,4)	145 (80,6)	180 (100,0)	
Regarding university degree				
With	25 (12,4)	176 (87,6)	201 (100,0)	<**0,001**
Without	104 (24,6)	319 (75,4)	423 (100,0)	
Regarding experience in e-mail usage				
Only one address	47 (24,0)	149 (76,0)	196 (100,0)	0,181
More addresses	82 (19,3)	343 (80,7)	425 (100,0)	

*Chi-square Test

There is also great need for developing one validated questionnaire as international measurement tool which can be used as basis for future empirical studies in area of information security user's awareness, for both scientific and professional community [18]. That questionnaire should be much more universal and not only password - oriented.

5 CONCLUSION

Starting premise is partly confirmed as both users with technical background knowledge and more experience have significantly better password quality, but regarding password usage (keeping password secret) those users were not better that users without technical background knowledge or with less experience. Moreover, users with technical background knowledge reuse the same password to access to more different information systems significantly oftener than users without technical background knowledge.

Users that need to access to more different information systems often reuse the same password(s). Although it is less insecure to use the same password of a good quality for several different systems than to use several passwords of a poor quality for each system, it is still potential information security breach. As if a same password is used for more systems, even a good one, when that password eventually gets stolen, cracked or hashed automatically will all those systems become compromised.

In results there was also unexpected statistical significance found regarding age for all questions and regarding university degree for questions about lending password or writing it down.

Young users have passwords of better quality. They are not lending their password and are not writing it down somewhere for remembering as older users, but they use the same password to access to more different information systems significantly oftener than older users. It is similar situation as with users that have technical background knowledge.

Although it does not have to be a big security issue if the password that is written down is safely deposited, it is still more secure not to write password down anywhere, but to remember it. This can be in contradiction with previous security requirement to have different password for each system, especially for users that need to access to a lot of different information systems. However, summary results had shown that small amount of users, not more than 20%, wrote their password down for remembering while opposite result is regarding reuse of the same password for accessing to more different information systems. More than half of examined users prefer to use the same password.

Summary results had also shown that small amount of users graded their passwords as *poor* (14%), and that small amount of users lent their password (20%). But disclosing password and having simple, easy-to-guess password are maybe the most critical password security issues analyzed in this paper. Those summary results are showing irresponsible behavior among certain amount of users regarding information security issues.

Although users can be quite aware of the password's importance they rarely follow security procedures and guidelines. Privacy or confidentiality with secrecy and good quality (or high complexity) are most important properties of a password, because if compromised password can cause loss of information as possibly most important business asset or personal value.

Results of this study highlighted importance of the security procedures and guidelines and need of the continuous education on security issues with constant informing and alerting of information systems' users. This study is an example on how to evaluate different users' security awareness in order to adjust courses on security issues and also how to adapt informing and alerting to different groups of information systems' users.

Possible drawbacks of this study are: focusing only on the password for e-mail system, high users' subjectivity in self-assessment and high authors' subjectivity when categorizing users regarding potential technical background.

Research should be repeated on the passwords used for "more important" information systems, especially regarding PINs for bank accounts. Maybe results will show more security awareness among users when personal bank account is the subject.

Plan for future work is to try to develop and validate universal questionnaire for ongoing empirical studies of this kind.

ACKNOWLEDGMENT

Author would like to thank to unknown reviewers on detailed and constructive suggestions for corrections. Also many thanks go to our mentor, professor Franjo Jovic.

REFERENCES

[1] K. Solic, K. Nenadic and D. Galic, "Empirical study on correlation between user's awareness and information security", *IJECES*, vol. 3, no. 2, 2012.

[2] State of Spam & Phishing - A Monthly Report. *Symantec*, URL: http://www.symantec.com/content/en/us/enterprise/other_resources/b-state_of_spam_and_phishing_report_12-2010.en-us.pdf, 2010.

[3] M. Williams, "Adventures in implementing a strong password policy", *SANS Security Essentials*, June 16, 2003.

[4] Hashcat advanced password recovery, URL: http://hashcat.net/oclhashcat-plus/, 2012.

[5] John the ripper password cracker, URL: http://www.openwall.com/john/, 2012.

[6] Indiana university passphrase policy and strength estimation, URL: http://kb.iu.edu/data/acpu.html, 2013.

[7] KeePass Password Safe, free opensource password manager, URL: http://keepass.info/, 2013.

[8] Apple's iCloud Keychain password management tool, URL: https://www.apple.com/support/icloud/keychain/, 2013.

[9] ISO/IEC 27001, Information security management systems - Requirements, 2013.

[10] J. A. Cazier, C. M. Botelho, Â„Password Collection through Social Engineering: An Analysis of a Simulated Attack", *Journal of Information System Security*, vol 6, no. 4, pp. 53–70, 2010.

[11] Password Calculator, URL: http://lastbit.com/pswcalc.asp, 2011.

[12] K. Solic, F. Jovic, D. Blazevic, “An approach to the assessment of potentially risky behaviour of ICT systems’ users”, *Tehnički vjesnik*, vol. 20, no. 2, pp. 335-342, 2013.

[13] M. Dell’Amico, P. Michiardi, Y. Roudier, “Password Strength: An Empirical Analysis”, *Proceedings IEEE INFOCOM*, (San Diego, CA) pp. 1-9, March 2010.

[14] A.G. Voyiatzis, C.A. Fidas, D.N. Serpanos, N.M. Avouris, “An Empirical Study on the Web Password Strength in Greece”, *15th Panhellenic Conference on Informatics*, (Kastonija Greece), pp. 212-216, Sept.-Oct. 2011.

[15] W. Ma, J. Campbell, D. Tran, D. Kleeman, “Password Entropy and Password Quality”, *4th International Conference on Network and System Security*, (Melbourne, VIC), pp. 583-587, 1-3, Sept. 2010.

[16] P.G. Kelley, S. Komanduri, M.L. Mazurek, R. Shay, T. Vidas, L. Bauer, N. Christin, L.F. Cranor, J. Lopez, “Guess Again (and Again and Again): Measuring Password Strength by Simulating Password-Cracking Algorithms”, *IEEE Symposium on Security and Privacy*, (San Francisco, CA), pp. 523 - 537, May 2012.

[17] S.J. Lukasik, Â„Protecting Users of the Cyber Commons“, *Communications of the ACM*, vol 54, no. 9, pp. 54-61, 2011.

[18] R. E. Crossler, A. C. Johnston, P. B. Lowry, Qing Hu, M. Warkentin and R. Baskerville, “Future directions for behavioral information security research” *Computers&Security*, vol 32, no. 1, pp. 90–101, 2013.

Krešimir Šolić received his Ph.D. from Faculty of Electrical Engineering, Osijek, Croatia. He is currently employed as a senior researcher at Faculty of Medicine and as consultant at ANSY. His scientific research and professional work deals generally with information security with special focus on user’s security awareness. His current occupation at work is statistical analysis in biomedicine while his research and consulting area is security assessment of information and computer systems with focus on evaluation of users’ security awareness followed with their training and education. He has published several papers in various international journals and conferences. List of published papers and detailed CV can be found on his personal web site at http://www.mefos.unios.hr/ kresimir/. Krešimir was student member of IEEE and is member of HDMI (Croatian Society for Medical Informatics) as part of European Association for Medical Informatics and International Medical Informatics Association; HBMD (Croatian Society for Biostatistics) and CroRec as part of EuroRec Institute. He is happily married and has twins Ana and Marko.

Hrvoje Očevčić received his M.Sc. from Faculty of Electrical Engineering, Osijek, Croatia. He is currently employed as a senior internal auditor of information systems at Hypo Alpe-Adria-Bank. He deals with information security and risk assessment of information systems. He has published several papers in various international journals and conferences. His research interests include risk assessment, business continuity management, information classification, incident management and generally information security. He is currently working on completing of doctoral thesis on the topic of decision support systems in the management of information systems.

Damir Blažević received his B.E. degree in electrical engineering in 2001, degree master of sciences in electrical engineering, was received in 2006, and Ph. D. degree in electrical engineering, telecommunications and informatics was received in 2012, all at the Faculty of Electrical Engineering in Osijek, Croatia. He is a member of the Croatian Chamber of Architects and Engineers in Construction since 2007. Member of several Technical Committees of the Croatian Standards Institute. Participates in teaching undergraduate and graduate level at Faculty of Electrical Engineering Osijek. Worked as Instructor at the Academy of networking technologies and a lecturer at seminars for professional development at ETF Osijek. He is currently working as a lecturer at Faculty of Electrical Engineering in Osijek. His research interests include computer networks, expert and intelligent systems.

AUTHORS’ ADDRESSES

Krešimir Šolić, Ph.D.
Faculty of Medicine,
Josipa Huttlera 4, 31 000 Osijek
email: kresimir@mefos.hr

Hrvoje Očevčić, M.Sc.
Hypo Alpe-Adria-Bank d.d.,
Slavonska avenija 6, Zagreb, Croatia
email: ocevcic@gmail.com

Damir Blažević, Ph.D.
Faculty of Electrical Engineering,
Kneza Trpimira 2B, 31000 Osijek, Croatia
email: damir.blazevic@etfos.hr

Received: 2013-05-31
Accepted: 2014-03-25