Empirical Study on the Correlation between User Awareness and Information Security

Case Study

Krešimir Šolić
J. J. Strossmayer University of Osijek,
Faculty of Medicine, Department of Biophysics, Medical Statistics and Medical Informatics
Josipa Huttlera 4, Osijek, Croatia
kresimir@mefos.hr

Krešimir Nenadić
J. J. Strossmayer University of Osijek,
Faculty of Electrical Engineering, Department of Computer Science
Kneza Trpimira bb, Osijek, Croatia
kresimir.nenadic@etfos.hr

Dario Galić
J. J. Strossmayer University of Osijek,
Faculty of Medicine, Department of Biophysics, Medical Statistics and Medical Informatics
Josipa Huttlera 4, Osijek, Croatia
galic@mefos.hr

Abstract *– There are many existing high quality technical security solutions, but ongoing cyberwar is still not suppressed, which implies that there is a need for new concepts in information security. It is possible that the problem persists because the existing technical solutions have not included human factors. Those solutions are mostly focused on the attacker but should also be focused on the user as the integral part of the safeguarded system. It is possible that the user presents the weakest element in the security chain as the internal treats are among the most frequent information security issues. In this paper the authors analyse empirical data collected by simulation of e mail user behaviour caused by their level of security awareness. Results of this study confirm hypotheses that users can significantly influence the overall information system security level as well as private and business data used in e mail communication. The aim of this paper is to stress the problem of human influence on the information system security among technicians involved in developing technical security solutions, such as software engineers developing new algorithms for spam filters.*

Keywords *– information security, information system, security awareness, user behaviour*

1. INTRODUCTION

Today the Internet is present in most of person's private and business activities and the border between real and virtual worlds gets blurrier with each passing day. This *virtual* world is becoming reality for most of the people in the world and in that way the importance of information security becomes equivalent to physical protection in the *real* world.

In order to protect data it is necessary to insure secure communication channels used for data transfer, to protect databases placed on file servers and to control or influence users that possess and use those data. Technical security solutions for physical and software protection with security procedures for redundancy and automation of backing-up are on a high quality level, but ongoing cyberwar is still not suppressed. A possible reason for this may be technical security solutions, because they rarely include the influence of the human factor on the system security level.

The human factor is considered to be probably the weakest element in the security chain because the internal threat is among the top information security issues [1].

There is a lack of empirical research within the academic field of IT security that tries to measure the amount of human influence [2]. Some existing empirical studies analyse user perception, behaviour and attitude towards computer ethics and information security [3-5], as computer security and computer ethics are important components of the management information system [6].

Future solutions should be focused on rising user security awareness by developing a certain level of distrust towards the unknown in the so-called *virtual reality* [7, 8]. This can be accomplished by applying a learned behaviour from the *real* world to the *virtual* one, in the way that passwords are kept secret, systems are logged-out and antivirus software is updated; just like entrance doors are locked when leaving, wallets and personal documentation are guarded well in pockets or handbags and there is a basic level of distrust towards unknown persons.

In this paper the authors analyse empirical data collected by simulation on e-mail user behaviour in order to evaluate significance of user impact on information security. Unwanted mail can be spam, viruses, trojans, worms or phishing. The most dangerous ones are direct phishing attacks that are frequently focused on middle level business management and private users [9]. More unwanted mail in user inboxes implies a greater potential security risk as there is a higher probability that in time users will eventually be *phished* compromising thereby their personal and company data.

The initial premise is as follows: a person as both an integral component and a user of an information system with potentially risky behaviour defined by the level of security awareness, can influence directly data security and indirectly the overall security of the information system.

2. SIMULATION DESIGN

Simulation was designed and based on the usage of the e-mail system by simulating different e-mail user behaviours, i.e. careful and security aware users versus security naive and uninformed e-mail users. Hypothetic questions aimed at the following:

- Is there going to be more unwanted mail because of user risky behaviour (e.g. questionable registrations around the World Wide Web) [10]?
- Is there going to be more unwanted mail because users leave their addresses around on the Internet [11]?
- Does it hold that even a careful e-mail user is obligated to eventually start receiving unwanted mail?

The authors made four groups of new e-mail accounts only for the purpose of this simulation. Each group of addresses was used during the simulation period of one calendar year. Different ways of usage are listed below:

- The first group was made up of 17 e-mail accounts and can be called Common Group as addresses were used for regular/usual e-mail communication;
- The second group made up of 18 e-mail accounts was called *Registration Group* and those addresses were used for registration on different Internet services;
- The third group was made of 12 e-mail accounts, it was called Web Page Group and those e-mail addresses were listed on the web site [16];
- The last group that was made of 18 e-mail accounts can be called Control Group and those addresses were not used at all.

Each e-mail account in one address group was opened on different e-mail services with different Internet domains or in different businesses, companies or educational institutions.

E-mail addresses that belonged to the *Common Group* were used in order to simulate a careful and security aware e-mail user. Those addresses were used approximately every second week for the whole simulation period in order to simulate common e-mail communication, by sending and receiving e-mails with real e-mail users who were mostly authors' associates.

With e-mail addresses from both the *Registration Group* and the *Web Page Group* authors simulated uninformed and naive e-mail users with their risky behaviour. Addresses from the *Registration Group* were used for registration purposes, approximately every second week of the simulation period, to different kinds of Internet services (e.g. investment organisations, webshop sites, forums, torrent sites, etc). After registration, authors activated each of the addresses and logged into each of the Internet services at least once.

The *Web Page Group* was made of e-mail addresses listed on the web page called *SpamCollector* that was made particularly for study purposes [12]. On this web page, there was a short description of the study and the contact details of the authors. Syntax of the listed addresses was the true raw e-mail address with an active link in order to be found by spamming software that are scanning the Internet in search of e-mail addresses. The web page was registered through Google registration service and linked from the main page of the institution's web site.

The last group of e-mail addresses called the *Control Group* was not used in any way. This group was made for control purposes only. In case there was some unwanted mail received on one of those addresses, it would mean that there was some kind of a problem with that domain (e.g. a hacked e-mail server, stolen back-up, etc.).

Statistical analysis was conducted with STATISTICA 10.0 (StatSoft Int. Tulsa, OK, the USA) software tool. Results are presented as the arithmetic mean with the total range of distributed data. Statistical nonparametric tests were used with a significance level defined as $\alpha=0.05$. The significant difference between groups is confirmed if $p<\alpha$.

3. RESULTS

Empirical data were absolute frequencies presenting the amount of unwanted mail received per each e-mail address. Data were collected by counting in two different time periods. It was collected first during the first year, which was the simulation period, and second during the second year while there was no simulation activity. Results presented in Table 1 are arithmetic mean numbers ranging from the minimum to the maximum of unwanted mail received per address in each group.

Table 1. Distribution of unwanted mail received among groups of e-mail addresses

	Average unwanted mail received per address /mean (min-max)		
Groups of e-mail addresses	During simulation period	Year after simulation period	Total period
Common Group	0.63 (0-3)	1.05 (0-4)	1.45 (0-4)
Registration Group	17.17 (6-124)	21.33 (3-78)	27.14 (3-124)
Web Page Group	15.58 (0-31)	26.58 (0-53)	21.08 (0-53)
Control Group	0.00 (0-0)	0.00 (0-0)	0.00 (0-0)

The nonparametric Kruskall-Wallis Test was used for statistical analysis for all three groups of e-mail addresses. This test was chosen because of a small number of e-mail addresses used and questionable normality of data distribution. The statistical test found a significant difference with respect to the amount of unwanted e-mail received between the *Common Group*, the *Registration Group* and the *Web Page Group* with p<0.001.

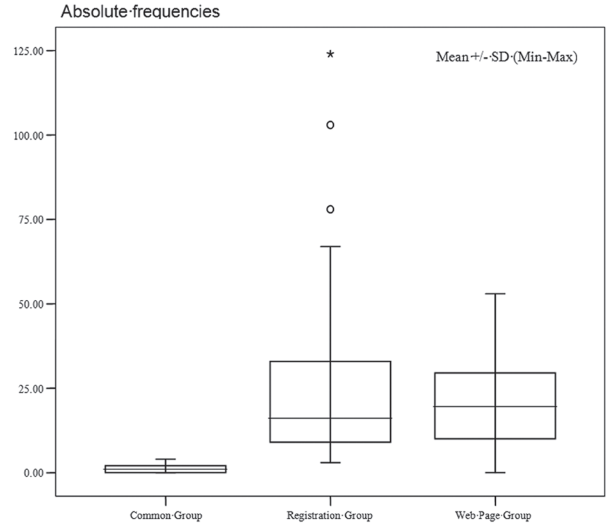

Fig. 1. The total amount of unwanted mail received per group (p<0.001)

The nonparametric Mann-Whitney U Test was used for statistical analysis for two groups of e-mail addresses with a small number of e-mail addresses used and questionable normality of data distribution. The statistical test did not find any significant difference with respect to the amount of unwanted mail received between the *Registration Group* and the *Web Page Group* with p=0.786.

Both the *Registration Group* and the *Web Page Group* present naive behaviour and they received a similar amount of unwanted mail, i.e. much more than e-mail addresses belonging to the *Common Group*, with a strong statistical significance (Fig. 1).

During the first few months of the simulation period there were only few unwanted mails received in the Registration Group, and none in other groups. In the Web Page Group of e-mail addresses there were no unwanted mails received before the web page became searchable through Google. Also, unwanted mail continued coming into inboxes, even when simulation actions stopped after first year. The ratio of unwanted mail received on average per account per month between address groups is illustrated in Fig. 2.

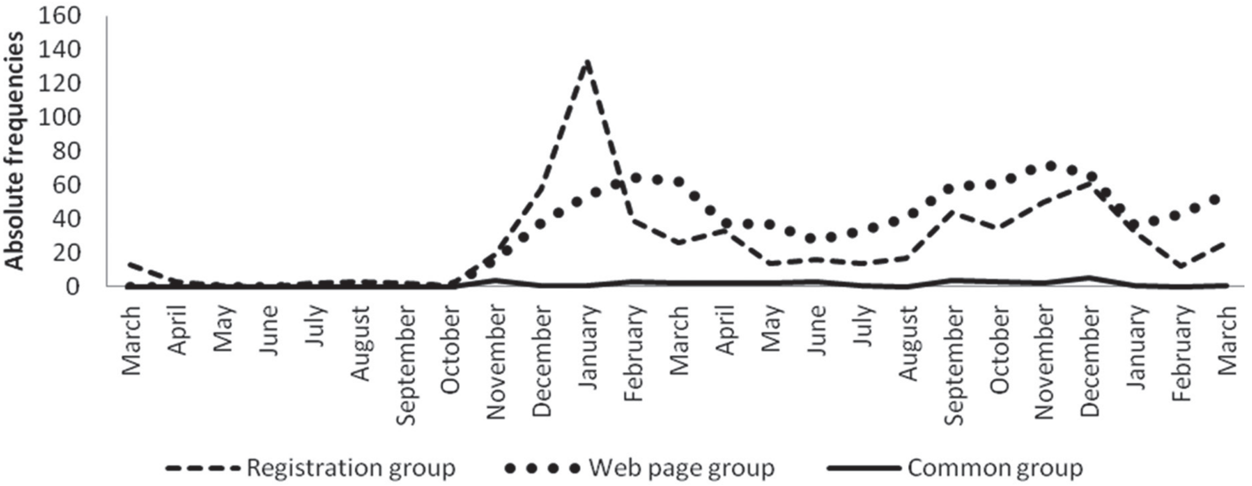

Fig. 2. Proportion of unwanted mail received during the test period

4. DISCUSSION

Results of this simulation confirmed all three hypothetic questions of this empirical study.

There will be significantly more unwanted mail in user inboxes if that user is not careful while using e-mail systems. Unfortunately, it seems that eventually every e-mail user will start to receive unwanted mail but if the user is aware and careful its amount is going to be reduced to a significantly lower level. Also, it seems that an e-mail address becomes corrupted for good by getting onto spammers' lists.

As most of security breaches into information systems are done through e-mail communication and by downloading files from the Internet, these results also confirm the initial premise: human as the integral component and as the user of an information system, can significantly influence security of utilised data, on the personal privacy, and the overall system security level.

5. CONCLUSION

This study has proven a significant correlation between user awareness of security issues and the overall information security level. Results also imply that technical security solutions are not enough for securing the information system if they lack an element that regulates human factor. If user awareness regarding security treats is better, a negative impact of their behaviour on the overall system security should be lower. This implies that additional security solutions should be focused on rising user security awareness. Some of the existing solutions are security policies that include user behaviour [13, 14], periodic education for employees stated in security guidelines [15, 16] and interactive educational tools for rising user awareness [8, 17, 18]. In the near future what can also be expected is development of technical solutions that will include control and blocking of the user potentially risky behaviour.

A drawback of this research can be a relatively low number of e-mail accounts opened per each address group, and there was also a problem with activation codes for some e-mail domains during registration on some of the used Internet services. Some e-mail services have stronger spam filters and for more general results the study should include other subsystems of the information system and comprise other aspects of human influence on the overall information security.

As empirical studies are not often in computer science, results of this study cannot be directly compared to previous similar, but rare, empirical studies.

Another problem is that studies of human behaviour fall under psychology, particularly under behavioural science. However, it is an ongoing problem in securing the computer information system omitting the user of the system as its constitutive element. However, there are some studies analysing information system user behaviour, possibly in cooperation with psychological associates [19-25].

Results of this study can be used to stress the problem of human influence on the information system security to technicians involved in developing technical security solutions, especially to software engineers developing new algorithms for spam filters.

6. REFERENCES

[1] I. Okere, J. Van Niekerk, M. Carroll, "Assessing information security culture: A critical analysis of current approaches", Proc. of Information Security for South Africa (ISSA), August 2012, pp.1-8.

[2] L. Ngo, W. Zhou, A. Chonka, J. Singh, "Assessing the level of IT security culture improvement: Results from three Australian SMEs", Proc. of Industrial Electronics (IECON) 35th Annual Conference of IEEE, November 2009, pp. 3189-3195.

[3] M. Aliyu, N.A.O. Abdallah, N.A. Lasisi, D. Diyar, A.M. Zeki, "Computer security and ethics awareness among IIUM students: An empirical study", Proc. of Information and Communication Technology for the Muslim World (ICT4M), December 2010, pp. A52-A56.

[4] T. Takemura, "Empirical Analysis of Behavior on Information Security", Proc. of Internet of Things (iThings/CPSCom), 4th International Conference on Cyber, Physical and Social Computing, October 2011, pp. 358-363.

[5] M. May, G. Fessakis, A. Dimitracopoulou, S. George, "A Study on User's Perception in E-learning Security and Privacy Issues", Proc. of 12th International Conference on Advanced Learning Technologies (ICALT) IEEE, July 2012, pp. 88-89.

[6] M. Masrom, Z. Ismail, "Computer security and computer ethics awareness: A component of management information system", Proc. of International Symposium on Information Technology (ITSim) IEEE, Vol. 3, August 2008, pp. 1-7.

[7] S.J. Lukasik, "Protecting Users of the Cyber Commons", Communications of the ACM, Vol. 54, No. 9, 2011, pp. 54-61.

[8] S. Furman, M. Theofanos, Y. Choong, B. Stanton, "Basing Cybersecurity Training on User Perceptions", IEEE Sec & Privacy, Vol. 10, No. 2, 2011, pp. 40-49.

[9] State of Spam & Phishing - A Montly Report, Symantec, http://www.symantec.com/content/en/us/enterprise/other_resources/b-state_of_spam_and_phishing_report_12-2010.en-us.pdf (9 September 2012).

[10] The 25 Most Common Mistakes in Email Security, IT Security, http://www.itsecurity.com/features/25-common-email-security-mistakes-022807/ (9 September 2012).

[11] G. Schryen, "The impact that placing email addresses on the Internet has on the receipt of spam - An empirical analysis", Computers & Security, Vol. 26, No. 5, 2007, pp. 361-372.

[12] SpamCollector, authors' web page, www.mefos.hr/dkts/ (9 September 2012).

[13] J. VanderMeer, "Seven Highly Successful Habits of Enterprise Email Managers - Ensuring that your employees' email usage is not putting your company at risk", Information Systems Security, December 2006, pp. 64-75.

[14] E.G. Park, N. Zwarich, "Canadian government agencies develop e-mail management policies", Int. J. Inform. Manag., Vol. 28, No. 6, 2008, pp. 468-473.

[15] The new users' guide - How to raise information security awareness, ENISA, http://www.enisa.europa.eu/activities/cert/security-month/deliverables/2010/new-users-guide (9 September 2012)

[16] IT Security Guidelines. Federal Office for Information Security, Bonn. https://www.bsi.bund.de/EN/Topics/ITGrundschutz/ITSecurityGuidelines/itSecurityguidelines_node.html (9 September 2012).

[17] L.V. Mangold, "Using Ontologies for Adaptive Information Security Training", Proc. of Seventh International Conference on Availability, Reliability and Security (ARES), August 2012, pp. 522-524.

[18] H. Kruger, W. Kearney, "A prototype for assessing information security awareness", Computers & Security, Vol. 25, No. 4, 2006, pp. 289-296.

[19] I. Androulidakis, G. Kandus, "Bluetooth® usage among students as an indicator of security awareness and feeling", Proc. of ELMAR, September 2011, pp. 157-160.

[20] A. Marks, Y. Rezgui, "A Comparative Study of Information Security Awareness in Higher Education Based on the Concept of Design Theorizing", Proc. of International Conference on Management and Service Science (MASS), September 2009, pp. 1-7.

[21] N. Yoshikai, S. Kurino, A. Komatsu, D. Takagi, M. Ueda, A. Inomata, H. Numata, "Experimental Research on Personal Awareness and Behavior for Information Security Protection", Proc. of 14th International Conference on Network-Based Information Systems (NBiS), September 2011, pp. 213-220.

[22] C. Li Jun, "Complex Network Community Structure of User Behaviors and Its Statistical Characteristics", Proc. of Third International Conference on Multimedia Information Networking and Security (MINES), November 2011, pp. 366-370.

[23] Z. Tu, Y. Yuan, "Understanding User's Behaviors in Coping with Security Threat of Mobile Devices Loss and Theft", Proc. of 45th Hawaii International Conference on System Science (HICSS), January 2012, pp. 1393-1402.

[24] K. Solic, F. Jovic, D. Blazevic, "An Approach to the Assessment of Potentially Risky Behavior of ICT System's Users", Technical Gazette, Vol. 20, No. 2, 2013.

[25] K. Solic, B. Tovjanin, V. Ilakovac, "Assessment Methodology for the Categorization of ICT System Users Security Awareness", Proc. of 35th International Convention MIPRO, May 2012, pp. 1560-1564.