There are many variations of passages of Lorem Ipsum available

Original Scientific Paper / Review Paper / Case Study / Preliminary Communication

Name Surname

J. J. Strossmayer University of Osijek,

Faculty of Medicine, Department of Biophysics, Medical Statistics and Medical Informatics

Street, City, Country

mail@mail.hr

Name Surname

J. J. Strossmayer University of Osijek,

Faculty of Electrical Engineering, Department of Computer Science

Street, City, Country

mail@mail.hr

Name Surname

J. J. Strossmayer University of Osijek,

Faculty of Medicine, Department of Biophysics, Medical Statistics and Medical Informatics

Street, City, Country

mail@mail.hr

***Abstract*** – Contrary to popular belief, Lorem Ipsum is not simply random text. It has roots in a piece of classical Latin literature from 45 BC, making it over 2000 years old. Richard McClintock, a Latin professor at Hampden-Sydney College in Virginia, looked up one of the more obscure Latin words, consectetur, from a Lorem Ipsum passage, and going through the cites of the word in classical literature, discovered the undoubtable source. Lorem Ipsum comes from sections 1.10.32 and 1.10.33 of "de Finibus Bonorum et Malorum" (The Extremes of Good and Evil) by Cicero, written in 45 BC. This book is a treatise on the theory of ethics, very popular during the Renaissance. The first line of Lorem Ipsum, "Lorem ipsum dolor sit amet..", comes from a line in section 1.10.32.

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

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 behavior 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 analyze empirical data collected by simulation on e‑mail user behavior 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 behavior defined by the level of security awareness, can influence directly data security and indirectly the overall security of the information system.

1. Sed quis est vitae

Simulation was designed and based on the usage of the e‑mail system by simulating different e‑mail user behaviors, 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 behavior (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 behavior. 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 organizations, web-shop sites, forums, torrent sites, etc.). After registration, authors activated each of the addresses and logged into each of the Internet services at least once.

2.1. Solar energy potential in
 Pannonian part of Serbia and
 Croatia

The *Web Page Group* was made of e‑mail addresses listed on the web page called *Spam Collector* 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 (Stat Soft 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 α=0.05. The significant difference between groups is confirmed if p<α.

1. 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.** Aliquam venenatis dui vitae elit varius iaculis.

|  |  |
| --- | --- |
|  | 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.

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).



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

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.

1. References:

All references should be listed according to the examples provided below and should be listed in the order in which they appear in the text:

 Examples for books:

[1] S. Theodoridis, K. Koutroumbas, “Pattern Recognition, Fourth Edition”, 4th Ed., Academic Press, 2008.

[2] A. E. Eiben, J. E. Smith, “Introduction to Evolutionary Computing”, 2nd Ed., Springer-Verlag Berlin Heidelberg, 2015.

 Examples for book chapters:

[3] A. Massa, M. Pastorino, A. Randazzo, “The Differential Evolution Algorithm as Applied to Array Antennas and Imaging”, Advances in Differential Evolution, pp. 239-255, Springer Berlin Heidelberg, 2008.

[4] J. Dai, B. Huang, “Design Patterns for Cloud Services”, New Frontiers in Information and Software as Services, pp. 31-56, Springer Berlin Heidelberg, 2011.

 Examples for journal papers:

[5] L. A. F. Fernandes, M. M. Oliveira, “Handling Uncertain Data in Subspace Detection”, Pattern Recognition, Vol. 47, No. 10, 2014, pp. 3225-3241.

[6] C. Henaux, B. Nogarede, D. Harribey, “A New Concept of Modular Permanent Magnet and Soft Magnetic Compound Motor Dedicated to Widespread Application”, IEEE Transactions on Magnetics, Vol. 48, No. 6, 2012, pp. 2035-2043.

 Examples for conference papers:

[7] M. Kulisiewicz, T. Kajdanowicz, P. Kazienko, M. Piasecki, “On Sentiment Polarity Assignment in the Wordnet Using Loopy Belief Propagation”, Proceedings of the 10th International Conference on Hybrid Artificial Intelligence Systems, Bilbao, Spain, 22-24 June 2015, pp. 451-462.

[8] Q. Liu, Y. Guo, J. Wu, G. Wang, “Dynamic Grouping Strategy in Cloud Computing”, Proceedings of the 2nd International Conference on Cloud and Green Computing, Xiangtan, Hunan, China, 1-3 November 2012, pp. 59-66.

 Examples for technical reports:

[9] R. Storn, K. V. Price, “Differential evolution: A Simple and Efficient Adaptive Scheme for Global Optimization over Continuous Spaces,” International Computer Science Institute, Berkeley, USA, Technical Report TR-95-012, 1995.

[10] D. Karaboga, “An Idea Based on Honey Bee Swarm for Numerical Optimization”, Erciyes University, Engineering Faculty, Turkey, Technical Report TR06, 2005.

 Examples for web resources:

[11] C. Langton, Orthogonal Frequency Division Multiplexing, www.complextoreal.com (accessed: 2015)

[12] MathWorks, Create 2-D Graph and Customize Lines, http://www.mathworks.com/help/matlab/creating\_plots/using-high-level-plotting-functions.html (accessed: 2014)

 Examples for theses:

[13] V. Mancapa, “A General Genetic Algorithm for One and Two Dimensional Cutting and Packing Problems”, Nelson Mandela Metropolitan University, Faculty of Engineering, Port Elizabeth, South Africa, Master Thesis, 2008.

[14] A. J. Bennet, “Investigation of an Immune Algorithm and Differential Evolution to Study Folding of Model Proteins”, University of Birmingham, School of Chemistry, Birmingham, United Kingdom, PhD Thesis, 2009.

[15] T. Matić, “Improved Real-Time Algorithms for Biscuit Tile Defects Detection”,Josip Juraj Strossmayer University of Osijek, Faculty of Electrical Engineering, Osijek, Croatia, PhD Thesis, 2014. (in Croatian)