SOCIAL NETWORKS SECURITY ASPECTS. A TECHNOLOGICAL AND USER BASED PERSPECTIVES

АСПЕКТИ В СИГУРНОСТТА НА СОЦИАЛНИТЕ МРЕЖИ. ТЕХНОЛОГИЧНИ И ПОТРЕБИТЕЛСКИ ПЕРСПЕКТИВИ

Zlatogor Borisov Minchev

Institute of ICT/Institute of Mathematics & Informatics, Bulgarian Academy of Sciences
Sofia 1113, Acad. Georgi Bonchev Str., Block 25A, Room 116,
Phone: +359 2 979 66 31, E-mail: zlatogor@bas.bg

Златогор Борисов Минчев

Институт по информационни и комуникационни технологии /
Институт по математика и информатика, Българска академия на науките
София 1113, ул. Акад. Георги Бончев, Бл. 25А,Стая 116,
Тел.: +359 2 979 66 31, E-mail: zlatogor@bas.bg

Keywords: social networks, social engineering, modeling, psychophysiological validation, user emotions and behaviour

Ключовидуми:социални мрежи, социаленинженеринг, моделиране, психофизиологична валидация, потребителскиемоции и поведение

Резюме:Статията разглежда някои водещи аспекти от социалния инженеринг/реинженеринг, както от технологична, така и от потребителска гледна точка. Представен е модел, използващ парадигмата „обект-връзка“ и експертни знания, който е валидиран посредством психофизиологичен мониторинг на две фокус групи. Получените резултати показват предразположеност на потребителите към заплахи, породени от Web 2.0технологиите, по смисъла на манипулативния социален инженеринг/реинженеринг, и предоверяване към някои известни социални мрежи. Последното възможно да предизвика негативни промени в потребителското емоционално състояние и поведение.

Abstract: The paper describes some leading security aspects, related to social engineering/reengineering from both technological and users' based perspectives. A model, organized around Entity-Relationship paradigm and experts' knowledge for the problem, is presented and validated on the basis of psychophysiological monitoring amongst two focus groups. The achieved initial results have shown a predisposition to Web 2.0 technological threats by means of manipulative social engineering/reengineering, concerning the users and over trust in some famous social networks. This can produce negative changes in users' behaviour and emotional state.

1. INTRODUCTION

Nowadays the social networks phenomenon is encompassing a rather large scale, due to the fast progressing information technologies. Generally, the communication process between people dates back to the very first social organizational attempts of human beings [7]. What however is important to note today, is the scale influence, produced as a result of combining the Internet idea with mobile communications. This, in fact, could be considered and as the major generic instability generator, talking from system based perspective [11]. So, the modern IT based social networks, practically associated mainly with Facebook, Twitter and LinkedIn [14] have to be concerned with care, having more than a billion and a half users. An attempt for this has been recently done in the EU Network of Excellence SySSec [5] study on social networks [10]. Generally, from these authors' efforts, it can be concluded that modern social networks have a multiaspect security profile that encompasses both technologies and users. Whilst, the technological problems, concerning users' privacy (guaranteed to some extent with social snapshots, logins and plugins) are basically well systematized they only partially address the peculiarities, related to mouse gestures, typing speed, preferences, habits, behaviour and emotions dynamics. Finally, what should be specifically noted here, concerns the emotions and users' behaviour experimentally studied by a young Bulgarian team in the framework of NSF project DMU 03/22 [1].

Being complex enough, and at the same time an emerging threat [8], [12]social engineering/reengineering have to be treated carefully encompassing both technologies and users in social networks.

The aim of the present paper is to present a model of the social engineering process and an attempt for identification of potential obvious and hidden threats. Further on, some of the model findings have been experimentally validated and some of the results are shortly noted here.

2. THE MODEL

The social engineering model has been developed in I-SCIP environment [9] and is depicted on Fig. 1.

Generally, the model from Fig.1 encompases 'Users', 'Mediators' and a set of their possible activities representing model *entities* (Mediators: 'Friendship', 'Grouping', 'Entertainment', 'Events', 'Campaigns', 'Advertisments', all coloured in red round rectangles; Users: 'Expressing', 'Sharing', 'Searching', 'Group Behaviour', 'Networking', 'Creativity', 'Real Activities', 'Positions', all coloured in green round rectangles).

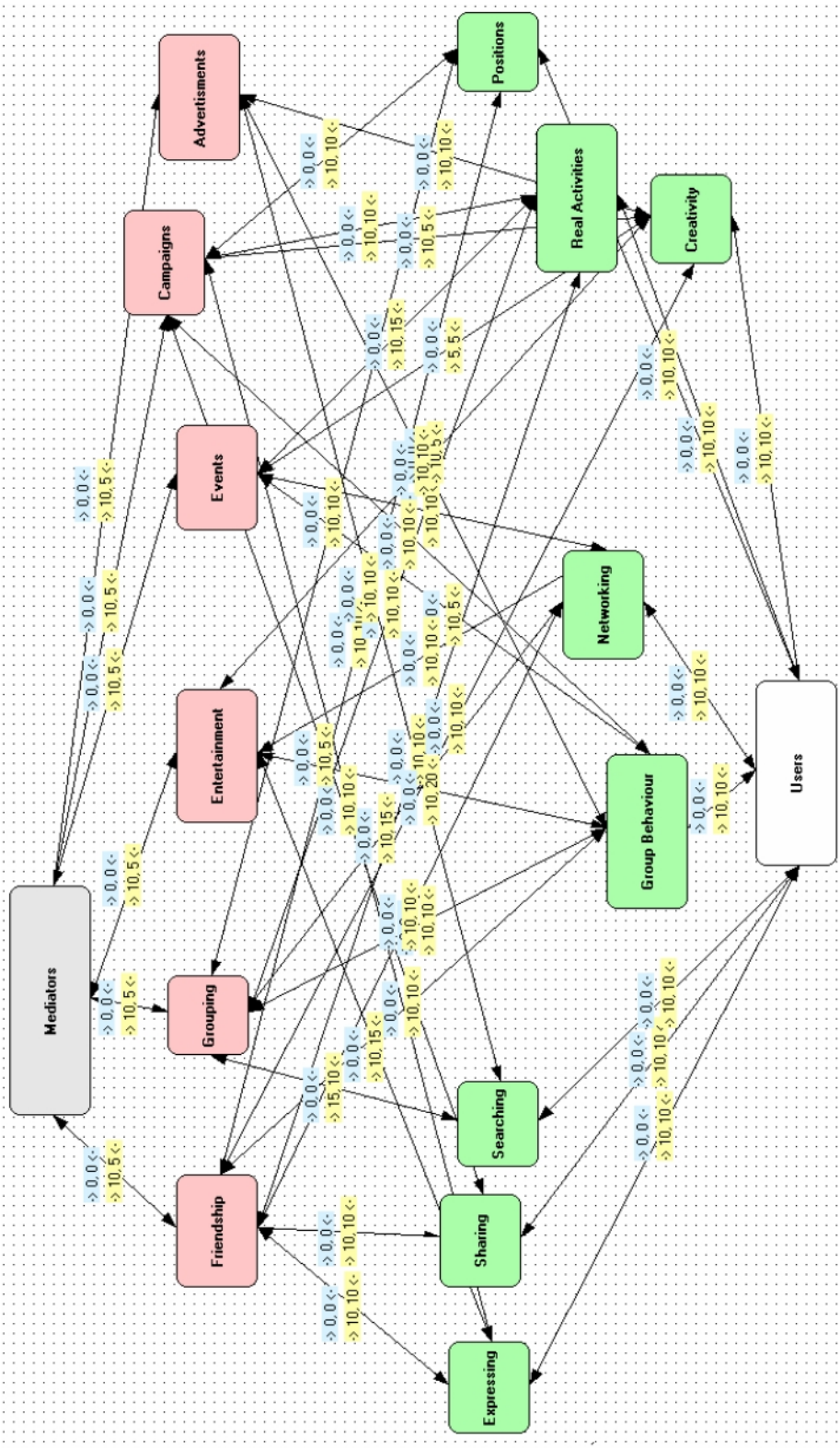

Fig.1. Social Engineering Model E-R interpretaion in I-SCIP environmnet.

The *relations* between entities are expressed with uni-/bi- directional headed arrows (weighted in percentages from the interval [0, 1] using the following scale: low [0-30], middle [30-50] and high [50-100], noted in yellow labels; the blue labels

on the arrows are concerning model's dynamics that is not included in the current model).The model development has been performed in I-SCIP v. 2.0 environment. Anice classificationof the model entities is producedin a resulting Sensitivity Diagram (SD) that uses and extends the ideas of Vester's sensitivity model [6], allowing model building elements' zone classification and system sensitivity analysis as follows: Red zone (active elements, Influence/Dependence Maximum Ratio (IDMR) =100/50, SE (South-East) part of SD cube), Blue zone (passive elements IDMR=50/100, NW (North-West) part of SD cube), Yellow zone (critical elements, IDMR=100/100, NE (North-East) part of the SD cube) and Green zone (buffering elements, IDMR=50/50, SW (South-West) part of SD cube). Additionally, the 3D SD gives a possibility for direct sensitivity (z-coordinate, marked with red arrow in Fig. 2) calculation of a given object from the system as an absolute difference between the influence (x-coordinate, marked with green arrow in Fig. 2) and dependence (y-coordinate, marked with blue arrow in Fig. 2) values, concerning a certain object from the system of interest. When this difference is negative the object in SD is classified as passive (producing a decreased system sensitivity in its SD zone) and is colored in light grey, otherwise it is active (producing an increased system sensitivity in its SD zone) and is colored in white.

The resulting SD, depicted on Fig.2, is agregating a set of experts' oppinions both for entities and relations weights gathered in the framework of: EU SySSec Network of Excellence Second Project Report on Threats on the Future Internet and Research Roadmap [12] and DMU 03/22, NSF Project [1] meeting discussions and training activities.

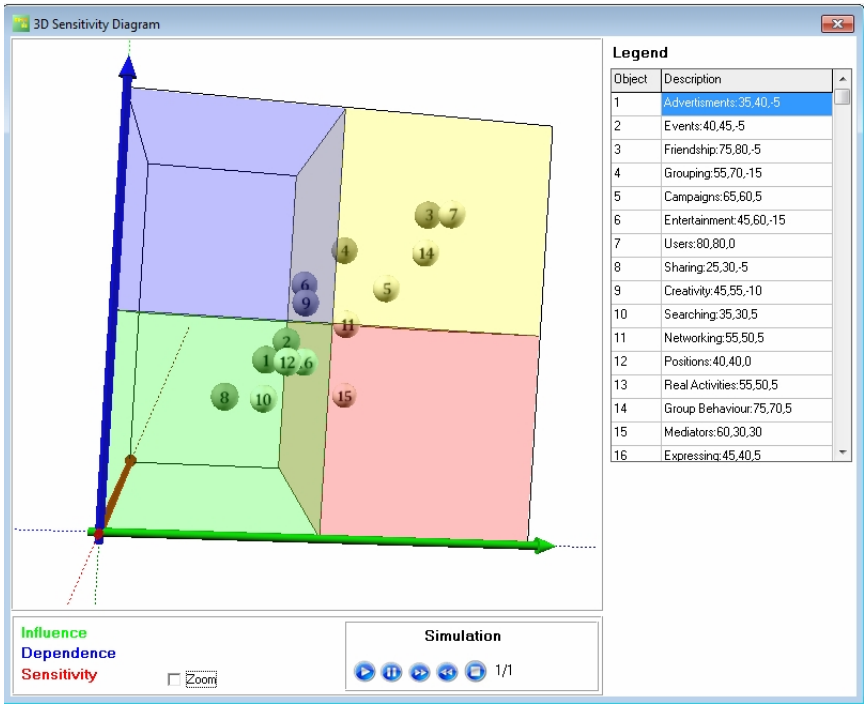

Fig.2. 3D Sensitivity Diagram of Social Engineering Model.

As it is clear from Fig. 2, four main clusters of entities are being produced: Active: 'Mediators'; Passive (Blue): 'Entertainment', 'Creativity'; Critical: 'Grouping', 'Friendship', 'Campaigns', 'Users', 'Group Behaviour', 'Networking' (though this entity together with its overlay 'Real Activities', is a boundary case between Active (Red) and Critical (Yellow) zones). The rest of the model entities have been classified as buffering (Green zone).

Whilst this classification is giving just entities 2D positions, we will try to give a better explanation of the results, taking into account the internal zones entities' roles ('active' – '+' vs 'passive' – '-'), their sensitivity (the z-coordinate in model SD) and the possible scenario context of explanation, concerning social engineering/reengineering.

First of all, special attention should be paid to: 'Entertainment' (z=-15), 'Grouping' (z=-15), 'Creativity' (z=-10) and 'Mediators' – (z =30), 'Positions' – (z=0), Users – (z=0). Additionally, in the present model it should be noted that the idea of equal importance regarding 'Mediators' vs 'Users' activities has been used. Finally, the relations evaluation has been performed with low weighted value in order to diminish the experts' evaluation noise and to accentuate on the entities and their relations as much as possible [9].

As a result of these a hypothesis that social engineering/reengineering is basically resulting success, due to the active role of 'Mediators', could be drawn.

But, special attention should be paid to 'Mediators' activities related to: 'Entertainment' and 'Grouping' possible hidden threats generators, keeping track on the 'Friendship' and 'Campaigns' that are from the Critical (Yellow) SD zone. 'Advertisements' and 'Events' activities of 'Mediators' are not concerned as influencing the 'Users' activities directly, though noted as 'passive' in the Buffering (Green) zone.

On the opposite side of the model – the 'Users' (which basically in the social reengineering case are 'Mediators') have to be watched for their 'Creativity' (Passive-Blue zone) by means of capability of building new applications with possible dual usage, i.e. hidden social reengineering.

3. **A VALIDATION ATTEMPT**

As far as the represented above social engineering/reengineering model relies basically on experts' opinions, a practical validation of the obtained results is good to be performed. In our present validation stage we have chosen a rather comprehensive one – the usage of psychophysiological monitoring of a focus group. Here it should be noted that this approach has been chosen in order to achieve a pretty near positioning to the target of social engineering/reengineering – the human factor and working at the same time with Web 2.0 technologies of nowadays social networks.

A group of 18 volunteers (15 men and 3 women, averaged age: 17.5 years), participants in the Summer School of Informatics, Varna Bulgaria, August 23-24,

2012 have been asked to fill-in a questionnaire of the most used social network (amongst Facebook, Twitter, Netlog and Youtube) in combination with the Zuckerman Sensation Seeking Scale [13].
The results have been aggregated around Fig. 3:

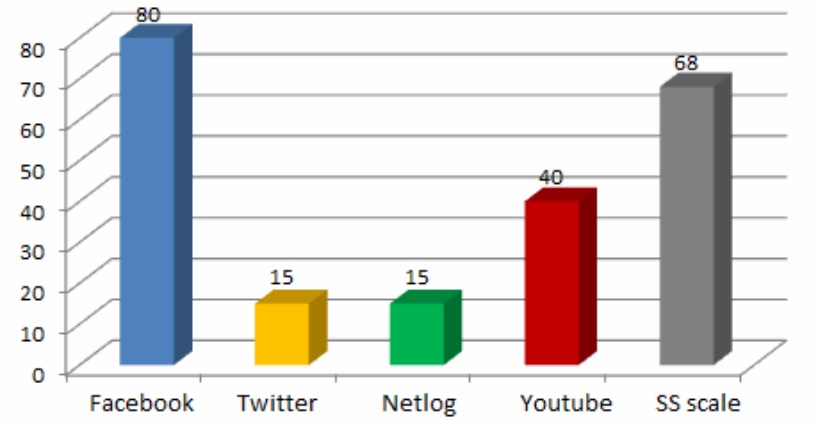

Fig. 3. Aggregated results from a focus group questionnaire survey of the most used social network (left) and Zuckerman Sensation Seeking Scale generalized results of the same group (right).

As this questionnaire based survey reported Facebook and Youtube as the most used social networks (the percentage is given for each social network, so the general sum is above hundred) and a nice average motivation for sensation seeking [13] amongst the volunteers we decided to organize a physiological monitoring of another focus group of 8 people (5 men and 3 women, average age: 28.6 years).We consider their reactions about famous social networks logos and names including Facebook, Twitter, Netlog and Youtube, but also and some others: LinkedIn, Wazzub, Google + and a distractor the Google search engine. All the participants were asked to fill-in and Von Zerssen Depression test [3] in order to understand their positive predispositions before the experiment (most of the participants have shown good results 5-10 points of this test [2]). For the physiological screening we used EEG recording from 6 positions (F3, F4, C3, C4, P3, P4 in accordance with International 10/20 system positioning) and a wireless polyphysiographicbluetooth equipment Nation 7128W-C20. The stimuli screens are depicted on Fig.4:

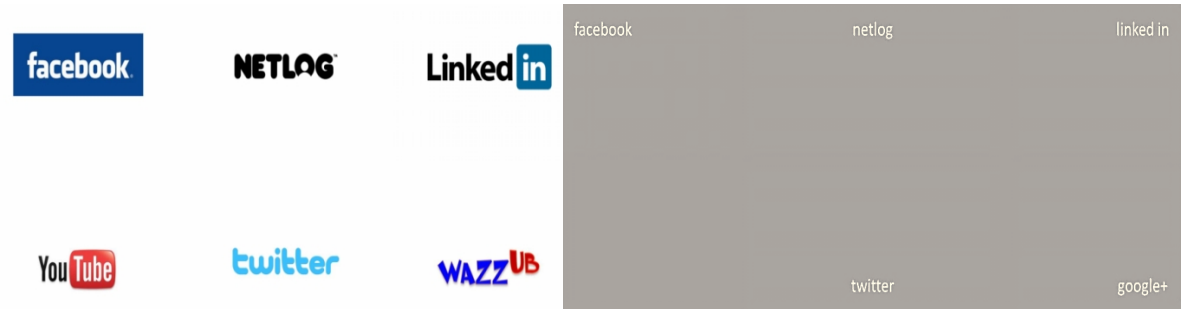

Fig.4. Stimuli screens with popular social network logos (left), names (right).

The aggregated results, regarding this study, and the event-related visual potentials have shown Facebook as the most emotional (by means of common arousal jump) brand and Twitter as the most emotional logo. The most significant reactions from the focus group members were noted about P300 (cognition ERP part) for Twitter and LinkedIn.

Finally, what could be speculatively (due to the small number of participants) concluded with these two psychophysiological experiments is the existence of predisposition to trust and like some of the social networks for the necessity of communication, achieving hidden depression overcoming [4]. Evidently this psychophysiological validation attempt gives a nice supplement to the model of social engineering/reengineering (see Section 2) roles of 'Mediators' and 'Users'.

4. DISCUSSION

The presented model for the emerging social engineering/reengineering in nowadays Internet space has shown some interesting results, regarding obvious and hidden threats for the nowadays social network users and the role of Web 2.0 technologies. Though the obtained results are achieved via experts' knowledge and small focus groups validation, the assumed methodology claims' closeness to the bigger trends of social engineering importance as a current and future cybersecurity problem. Finally, it is vital to note and the necessity of studying, both the technology and their users, in order to achieve better understanding how to get comprehensive security from both view points and to protect users, i.e. preparing for the upcoming Web 3.0 that will practically allow machines to take part in the social engineering/reengineering process.

5. ACKNOWLEDGEMENTS

This study was supported by: A Study on IT Threats and Users Behavior Dynamics in Online Social Networks, DMU03/22, Bulgarian Science Fund, Young Scientists Grant, 2011-2013, www.snfactor.com

A special gratitude is expressed for the expert and methodological support to:

EU Network of Excellence in Managing Threats & Vulnerabilities for the Future Internet – SySSec, under grant agreement n° 257007, 2010-2013, www.syssec-project.eu

Cortical Regulation of the Quiet Stance during Sensory Conflict, Project Grant TK 02/60, www.cleverstance.com

Finally, the author would like to thank personally to his colleagues Assoc. Prof. Plamen Gatev, MD and Assist. Prof. Stiliyan Georgiev from the Institute of Neurobiology, Bulgarian Academy of Sciences for the psychophysiological monitoring support and fruitful discussions.

6. REFERENCES

[1]. A Study on IT Threats and Users Behaviour Dynamics in Online Social Networks, DMU03/22, Young Scientists Project Web page, Available at: www.snfactor.com

[2]. D, Von Zerssen Depression Test, Available at: http://www.polls.hapche.bg/index.php?sid=22961

[3]. D., Zerssen, Von, F., Strian, & D. Schwarz, "Evaluation of depressive states, especially in longitudinal studies". In Psychological Measurements in Psychopharmacology (eds P. Pichot& R. Olivier-Martin), 189-203, Basel: Karger, 1974.

[4]. Cortical Regulation of the Quiet Stance during Sensory Conflict, I Stage Report, NSF Grant TK 02/60, Institute of Neurobiology, Bulgarian Academy of Sciences, June, 2012.

[5]. EU Network of Excellence in Manging Threats and Vulnerabilities for the Future Internet, SySSec Project Web Page, Available at: www.syssec-project.eu

[6]. F. Vester, "The Art of Interconnected Thinking", Report to the Club of Rome, May, 2002.

[7]. J. Lopez. and J. Scott, *Social Structure*, Buckingham and Philadelphia, Open University Press, 2000.

[8]. Z. Minchev, "ICT Cyber Security", In Problem space report: Critical infrastructure & supply chain protection, Focus Project Consortia, January, 2012, Available at: http://www.focusproject.eu/documents/14976/014b8126-d528-4b01-a73a-e56ecce70f74

[9]. Z. Minchev and M. Petkova, "Information Processes and Threats in Social Networks: A Case Study", In Conjoint Scientific Seminar "Modelling and Control of Information Processes", Organized by: College of Telecommunications, Institute of ICT - Bulgarian Academy of Sciences and Institute of Mathematics and Informatics – Bulgarian Academy of Sciences, Sofia, Bulgaria, November, 85-93, 2010.

[10]. Preliminary Report on Social Networks Security, SySSec Consortia, March 2012, Available at: http://www.syssec-project.eu/media/page-media/3/syssec-d5.2-SoA-SocialNetworkSecurity.pdf

[11]. R. Ashby, *An Introduction to Cybernetics*, Chapman & Hall Ltd., 1957.

[12]. Second Report on Threats on the Future Internet and Research Roadmap, SySSec Consortia, September, 2012, Available at: http://www.syssec-project.eu/media/page-media/3/syssec-d4.2-future-threats-roadmap-2012.pdf

[13]. Sensation Seeking Scale Test, Available at: http://www.rta.nsw.gov.au/licensing/tests/driverqualificationtest/sensationseekingscale/index.html

[14]. Top 15 Most Popular Social Networking Sites, September 2012, Available at: http://www.ebizmba.com/articles/social-networking-websites