Editorial: Special issue CISIS12-IGPL

The nine contributions selected in this special issue represent a collection of extended papers presented at the 5th International Conference on Computational Intelligence in Security for Information Systems (CISIS 2012).

CISIS aims to offer a meeting opportunity for academic and industry-related researchers belonging to the various, vast communities of *Computational Intelligence*, *Information Security* and *Data Mining*. The need for intelligent, flexible behaviour by large, complex systems, especially in mission-critical domains, is intended to be the catalyst and the aggregation stimulus for the overall event.

In the first contribution, Durán *et al.* analyse a new proposal for a knapsack-type cryptosystem, published by Wang and Hu, along with two cryptanalyses of it, carried out by Youssef and Lee. They also analyse another proposal for a combinatorial cryptosystem, written by the same authors, together with a cryptanalysis of it, authored by Xu *et al.* Both cryptosystems prove to be safe only if the keys have very large sizes, but this severely impacts the use of the systems from a practical point of view. Moreover, they also give evidence suggesting that the independence of the combinatorial system with respect to the integer factorization problem might not be so solid as claimed by the authors. Finally, they answer in the affirmative the open question about the computational complexity of the matrix combinatorial problem, by showing that it is solvable in polynomial time if the factorization of N is known.

In the next contribution, Laorden *et al.* developed a conversational agent (Negobot) posing as a child, in chats, social networks and other channels suffering from paedophile behaviour. As a conversational agent, Negobot has a strong technical base of Natural Language Processing and information retrieval, as well as Artificial Intelligence and Machine Learning. However, the most innovative proposal of Negobot is to consider the conversation itself as a game, applying game theory. In this context, Negobot proposes, first, a competitive game in which the system identifies the best strategies for achieving its goal, to obtain information that leads us to infer if the subject involved in a conversation with the agent has paedophile tendencies, while our actions do not bring the alleged offender to leave the conversation due to a suspicious behaviour of the agent.

In this contribution, Walkowiak et al. propose a survivable distributed computing system using the $1+1$ protection approach working as an overlay network built on top of an existing underlying communication network. Their proposal is thus in contrast to recent papers mainly related to Grid systems using a dedicated optical network to connect the computing sites. Since the considered optimization problem is NP-complete, apart from introducing the respective ILP model, they also provide two suboptimal offline metaheuristic algorithms, namely: AlgTS, based on the Tabu Search method, and AlgGen, based on the genetic algorithm, to obtain the results close to the optimal ones in a reasonable time. Extensive numerical experiments, conducted to verify the efficiency the heuristic approaches against the optimal results, confirmed the benefits of our proposals. In particular, the obtained optimality gap was as low as 5–7%, on average.

In this contribution, Chorás and Kozik focus on countering emerging application layer cyber attacks since those are listed as top threats and the main challenge for network and cyber security. The major contribution of the paper is the proposition of machine learning approach to model normal behaviour of application and to detect cyber attacks. The model consists of patterns (in form

Vol. 23 No. 1, © The Author 2015. Published by Oxford University Press. All rights reserved.
For Permissions, please email: journals.permissions@oup.com
doi:10.1093/jigpal/jzu041

of Perl Compatible Regular Expressions regular expressions) that are obtained using graph-based segmentation technique and dynamic programming. The model is based on information obtained from HTTP requests generated by client to a web server. They have evaluated our method on CSIC 2010 HTTP Dataset achieving satisfactory results.

In this paper, Varela-Vaca and Gasca propose a formalization of security controls based on security patterns templates and feature models. This formalization allows applying feature-domain-oriented analysis and constraint programming techniques for the automatic inference, selection and generation of optimal security controls with regard to single and multiple business objectives.

In this work, Delgado-Mohatar and Fúster-Sabater analyse the design and software implementation of Linear Feedback Shift Registers (LFSRs) defined over extended fields GF(2^n) instead of over the binary field GF(2). The key idea is combining algebraic structures (finite fields) with modern processor capabilities to take advantage of the underlying device over which the application is executed. The study has been carried out for diverse extended fields and different architectures. Detailed microanalysis and macroanalysis of the LFSR implementation are performed too. Numerical results prove that extended fields provide speed-up factors up to 10.15. The benefits of these fields are clear for applications with LFSR cryptographic applications.

In this work, Zelinka et al. demonstrate a novel way on how to identify the operating systems and networking devices working with Transmission Control Protocol/Internet Protocol stack on the basis of differences in their pseudorandom number generators. Data from pseudorandom number generators of various OS are used to be visualized for its randomness in 3D space, using reconstruction method from deterministic chaos. Then fractal geometry is applied to measure fractal dimension of observed 3D clouds and compared with Euclid objects and among themselves. Interesting fractal properties are revealed and discussed in this paper as well as sketch of possible OS identification based on fractal geometry and neural networks.

In this paper, Ksieniewicz et al. present a novel Hyperspectral Segmentation Algorithm, which is part of a general framework used for image classification. The algorithm is based on image decomposition into homogeneous regions using a novel similarity measure. Three different region representations are proposed using the matrix notation. An additional procedure merges similar regions into larger ones to reduce human expert engagement in region labelling. The algorithm has been evaluated on the number of benchmark datasets to investigate the influence of algorithm parameters on the final performance. Comparison with competing methods proved that the considered algorithm is an interesting proposition in hyperspectral image analysis tasks.

This study, by Sánchez et al. aims at being one step towards the proposal of an Intrusion Detection System (IDS) that faces those attacks not previously seen (zero-day attacks), by studying the combination of clustering and neural visualization techniques. To do that, MObile VIsualisation Connectionist Agent-Based IDS (MOVICAB-IDS), is upgraded by adding clustering methods. Present work proposes the application of clustering techniques to provide automatic response to MOVICAB-IDS to quickly abort intrusive actions while happening. To check the validity of the proposed clustering extension, it faces now an anomalous situation related to the Simple Network Management Protocol (SNMP): a community search. This attack to get the community string (password guessing) is analysed by clustering and neural tools, individually and in conjunction. Through the experimental stage, it is shown that the combination of clustering and neural projection improves the detection capability on a continuous network flow.

The guest editors wish to thank Professor Dov Gabbay, (Editor-in-Chief of *Logic Journal of the IGPL*) for providing the opportunity to edit this special issue. We would also like to thank the

referees who have critically evaluated the papers within the short time. Finally, we hope the reader will share our joy and find this special issue very useful.

Álvaro Herrero
Department of Civil Engineering, University of Burgos, Burgos, Spain
e-mail: ahcosio@ubu.es

Václav Snášel
VŠB-TU Ostrava, Ostrava, Czech Republic
e-mail: vaclav.snasel@vsb.cz

Ajith Abraham
Machine Intelligence Research Labs (MIR Labs)
Scientific Network for Innovation and Research Excellence, Auburn, Washington, USA
e-mail: ajith.abraham@ieee.org

Ivan Zelinka
VŠB-TU Ostrava, Ostrava, Czech Republic
e-mail: Ivan Zelinka ivan.zelinka@vsb.cz

Héctor Quintián
Universidad de Salamanca, Salamanca, Spain
e-mail: hector.quintian@usal.es

Emilio Corchado
Universidad de Salamanca, Salamanca, Spain
e-mail: escorchado@usal.es

Received 12 November 2014