Editorial: SPECIAL ISSUE CISIS13-IGPL

The nine contributions selected in this special issue represent a collection of extended papers presented at the sixth International Conference on Computational Intelligence in Security for Information Systems (CISIS 2013).

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 Peinado *et al*. propose a hash function designed to implement a content-based image authentication mechanism using self-organizing map (SOM) trajectories and sparse features extracted from images. The features computed are used as inputs to the SOM, which computes a number of prototypes. After that, the prototypes, corresponding to each image block, define a trajectory in the SOM space, which is used to define the hash. Moreover, the image transformations can be identified as they impose changes in hash. Authors found that trajectories computed using sparse features present a more stable behaviour with small SOMs.

In the next contribution, Fuentes *et al.* present the design and optimization of the input modules of a toolbox to carry out differential power analysis attacks against the physical implementation of a given cryptosystem. Text and key modules allow inputting the plaintext or cipher text to the targeted cryptographic algorithm and the corresponding hypothetical values about the used key, respectively. Once configured, the toolbox Power Traces module controls a digital oscilloscope, which acquires the power traces during the operation of the device and automatically performs the necessary traces alignment. It can also perform statistical operations with the stored values representing the acquired traces. An analysis about different object-oriented trace representation options to implement the toolbox is performed and results are presented.

In this contribution, Molina-Gil *et al*. present a practical analysis of the SNOW 3G generator used to protect the confidentiality and integrity in long-term evolution communications. In particular, several techniques to perform multiplications and linear feedback shift register operations have been studied and implemented on both iOS and Android platforms. The evaluation of those implementations led to some conclusions that could be used to improve the efficiency of future implementations of the standard.

In this paper, Galán-Garcia *et al*. present a methodology to detect and associate fake profiles on Twitter social network, which are employed for defamatory activities to a real profile within the same network by analysing the content of the comments generated by both profiles. Accompanying this approach it is also presented a successful real life use case in which this methodology was applied to detect and stop a cyberbullying situation in a real elementary school.

In the next paper, Cambiaso *et al*. focus on 'Denial of Service attacks' and specially on the so-called Slow DoS Attacks, which are able to reach their goal by using tiny amounts of network bandwidth. Authors designed an innovative offensive tool, SlowDroid, which may affect multiple protocols requiring minimal resources to the attacker. In virtue of this, the attack can even be executed from a mobile device. Authors compare the attack with similar already existing tools, measuring the results obtained based on new metrics and proving that the proposed threat represents a serious menace.

In this contribution, Álvarez and Zamora analyse the randomness properties of key-derived s-boxes generated by some popular cryptosystems like the RC4 stream cipher, and the Blowfish and Twofish

Vol. 24 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/jzv040   Advance Access published 18 November 2015

block ciphers with the aim of establishing if this kind of s-boxes are indistinguishable from purely random s-boxes. For this purpose authors have developed a custom software framework to generate and evaluate random and key-derived s-boxes. They also detail and analyse several mechanisms for the generation of proper key-derived s-boxes, including fixed point filtering and different sizes based on 8×8 s-boxes.

In next paper, Ventura *et al*. extend and analyse a previous access control solution for wireless network services with group-based authorization. Authentication and encryption are provided, and access control relies on user identity, group membership and time intervals. Both the basic solution and the extension focus on minimizing computation, energy, storage and communications on the sensor side: computations involved rely on symmetric cryptography and key derivation functions, and no additional messages between user and sensor are needed. The performance of author's solution is proven by experiments on a highly constrained platform such as Arduino. Finally, its security is validated against the AVISPA tool.

The aim of the next work, by Pintea *et al*., is to describe a new general defence mechanism, based on multi-agents in order to stop jamming attacks on wireless sensor network (WSN). It is analysed and discussed the reaction of artificial sensitive agents to several stigmergic variables in order to keep the tracks of intruders in a sensor network. As well, it is illustrated the way in which are detected and isolated the attacks using groups of agents based on direct communication. The proposed algorithm could be easily further extended to solve other security issues in networks and in particular for WSNs.

Final contribution, by González *et al*., addresses the detection of secure shell protocol (SSH) anomalous connections from an Intrusion Detection perspective. The main idea is to compare several strategies and approaches for a better detection of SSH-based attacks. To test the classification performance of different classifiers and combinations of them, SSH data coming from a real-world honeynet are gathered and analysed. For comparison purposes and to draw conclusions about data collection, both packet-based and flow data are analysed. A wide range of classifiers and ensembles are applied to these data, as well as different validation schemes for better analysis of the obtained results. The high-rate classification results lead to positive conclusions about the identification of malicious SSH connections.

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
University of Burgos, Burgos, Spain
E-mail: ahcosio@ubu.es

Bruno Baruque
University of Burgos, Burgos, Spain
E-mail: bbaruque@ubu.es

Ajith Abraham
Machine Intelligence Research Labs (MIR Labs), USA
E-mail: ajith.abraham@ieee.org

André C.P.L.F. de Carvalho
University of Sao Paulo, Sao Carlos, Brazil
E-mail: andre@icmc.usp.br

Pablo García Bringas
University of Deusto, DeustoTech Computing, Bilbao, Spain
E-mail: pablo.garcia.bringas@deusto.es

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 15 September 2015