Preface to Issue 4
"Security Systems, Cryptographic Protocols & Network Security"

Cryptography and security systems are two fields of security research that strongly interact and complement each other. The International Conference on Cryptography and Security Systems (CSS) is a forum of presentation of theoretical, applied research papers, case studies, implementation experiences as well as work-in-progress results in these two disciplines. The Conference especially invites young researchers and PhD students who have an opportunity to share their results with colleagues, invited lecturers and the Program Committee members who actively participate in conference sessions.

In the second edition of the International Conference on Cryptography and Security Systems (CSS 2012) 18 regular presentations (selected out of 25 submitted papers by the authors from 10 countries) and 3 general invited lectures have been presented. The first lecture was given by Dr. Pascal Lafourcade from the University of Joseph Fourier in Grenoble on "Automatic Security Proof of Cryptographic Primitives : Public Encryption, Symmetric Encryption Modes, MAC...". Dr. Lafourcade presented current results of his and co-workers' research on constructing a tool for automatic verification of correctness of cryptographic protocols and their security against common attacks. After presenting the background of his tool and formal description of protocols, he concentrated on the analysis of three groups of the most popular cryptographic primitives which are public-key cryptosystems, symmetric ciphers in different modes of operation and hash functions applied in the MAC protocols.

The second general lecture was presented by Dr. Mark D. Cole from the University of Luxembourg and its subject was "Combating Cybercrime - Can Law Contribute to Enhancing Security of Communication Networks? On International, European and National Responses and Possibilities". Dr. Cole presented current problems of fighting cybercrime from the point of view of individual countries' national, European and, generally, international legal regulations. This lecture initiated interesting discussion moved on for the coffee break since the audience understood that the fundamentals of any protection method should lie in good law and international agreements on rights and licenses as well as every day cooperation.

The third invited lecture was by Dr. Krzysztof Chmiel from Poznań University of Technology. Its title was "Methods of Differential and Linear Cryptanalysis of Block Ciphers". Dr. Chmiel gave an overview and the summary of his research on cryptanalysis of symmetric block ciphers, starting with the first attacks on the DES cipher and ending with the analysis of modern PP1 encryption algorithm. He also presented different approaches to estimation of security level of cipher and methods of approximations of the most complicated ciphers' component operations.

The regular papers accepted for CSS 2012 were presented during the sessions that can be grouped into two tracks. The papers included in Issue 4 of volume XII of Annales UMCS ser. Informatica belong to the track of CSS 2012 called "Security Systems, Cryptographic Protocols & Network Security". Alike Issue 3, this issue consists of 9 papers reflecting topical problems of security systems. The first three papers have the common topic which is application of artificial intelligence methods in secure systems and security protocols. The paper by Nicolas Bernard and Franck Leprévost entitled "Hardened Bloom Filters, with an Application to Unobservability" shows that the concept of hardened Bloom filters, combining classical Bloom filters with cryptographic hash functions and secret nonces, can be successfully used in the TrueNyms unobservability system and protects it against replay attacks. Vaidas Juzonis, Nikolaj Goranin, Antanas Cenys and Dmitrij Olifer in the paper "Specialized Genetic Algorithm Based Simulation Tool Designed For Malware Evolution Forecasting" deals with malware evolution forecasting providing an opportunity to predict malware epidemic outbreaks, developing effective countermeasure techniques and evaluating information security level. To achieve such an effect they apply a genetic algorithm approach. A method applied in various security solutions is the subject of the paper "Image Reconstruction With the Use of Evolutionary Algorithms and Cellular Automata" presented by Franciszek Seredynski, Jaroslaw Skaruz and Adrian Piraszewski. Two-dimensional, nine state cellular automata with Moore neighbourhood perform reconstruction of an image presenting a human face. Large space of automata rules is searched through efficiently by a genetic algorithm.

The next group of papers presented in CSS 2012 deals with formal and automated analysis of cryptographic protocols. The paper "Automatic Detection of DoS Vulnerabilities of Cryptographic Protocols" by Urszula Krawczyk and Piotr Sapiecha considers the problem of DoS vulnerabilities of cryptographic key establishment and authentication protocols. It introduces a system for computer-aided DoS protocol resistance analysis employing the Petri nets formalism and the Spin model-checker. The successive paper by Bogdan Księżopolski, Damian Rusinek, Adam Wierzbicki, "On the Modelling of Kerberos Protocol in the Quality of Protection Modelling Language (QoP-ML)" first presents an outline of the original QoP Modelling Language and next gives an example of its effective application for investigation of security and performance of Kerberos key distribution protocol.

The next three papers consider security issues in the distributed and P2P networks. The paper by Xiaobing He, Pawel Szalachowski, Zbigniew Kotulski, Nikos Fotiou, Giannis F. Marias, George C. Polyzos and Hermann De Meer entitled "Energy-aware Key Management in Mobile Wireless Sensor Networks" is the effect of NoE EuroNF founded E-Key-Nets project. In the paper, based on the Group Diffie-Hellman key agreement protocols and the energy level of each node in the network, new Energy Aware Group Diffie-Hellman key management protocols for mobile wireless sensor networks are proposed. The tests results show that the proposed key management protocols provide great improvement in maximizing the lifetime of the WSN. The paper of Grzegorz Oryńczak and Zbigniew Kotulski, "Notary-Based Self-Healing Mechanism for Centralized Peer-to-Peer Infrastructures" presents a method of avoiding disadvantages of a single point of failure vulnerability in the P2P centralized networks. High security level is obtained by using notary servers which track server public key changes and collect social feedback from the users. By incorporating a reputation mechanism in the case of failure the best candidates for a new Central Server can be elected. The last paper in this group, written by Marcin Alan Tunia, deals, as its title says, with "Distributed Social Network". It presents new architecture of social network, which provides mechanisms for dividing data between more than one entity and combining independent data repositories in order to deliver one social network with clearly defined interfaces used to connect new data sources.

Alike Issue 3, also in this issue the steganography problems are not neglected. The paper "Security Issues on Digital Watermarking Algorithms" by Wioletta Wójtowicz and Marek R. Ogiela considers watermarking of medical images and security of such a procedure. The Authors put emphasis on the advantage features of DWT such as local time-frequency and multi-scale analysis, keeping the quality of host image and ensuring high robustness of watermark and present three algorithms which are based on the combination of DWT and some other transformations like DFT, DCT and Arnold transform, evaluating their quality and security.

Zbigniew Kotulski
Bogdan Księżopolski