ENIGMA – Brazilian Journal of Information Security and Cryptography Volume 2 Issue 1 September 2015

E. T. Ueda, *Editor in Chief,* M. S. M. A. Notare, *Associate Editor in Chief,* and R. T. de Sousa Júnior, *Associate Editor in Chief*

***Abstract*— This is the first issue of Volume 2 of ENIGMA – Brazilian Journal of Information Security and Cryptography. Submissions were accepted in English, Portuguese and Spanish. In this issue, 6 papers are published, of which 3 were peer-reviewed while the other 3 were invited and reviewed by the editorial board of the Journal. In addition, one of the invited papers was the second Best Paper from the conference SBRC'2015 while another was the Best Paper of the conference SBSeg'2014.**

***Keywords*— Brazilian Journal, Cryptography, Information Security.**

I. INTRODUCTION

ENIGMA – Brazilian Journal of Information Security and Cryptography – is a technical-scientific publication that aims at discussing theoretical aspect contributions and practical applications results in information security, cryptography and cyber defense as well as fundamental subjects in support of those issues.

The choice of the name ENIGMA for this publication is related to the ENIGMA cryptography machine. However, the main reason for this choice is to pay tribute to the mathematician and computer scientist Alan Mathison Turing (1912-1954), considered one of the leading scientists in the history of computing.

This journal is directed to academia researchers, industry professionals, members of government and military organizations, and all people that have interest in the area of information security and cryptography in order to disseminate and share their new technologies, scientific discoveries and research contributions.

The creation of this periodical is due the necessity to solve a gap represented by the lack of a technical-scientific Brazilian journal that emphasizes information security and cryptography. In this manner, ENIGMA – Brazilian Journal of Information Security and Cryptography – must provide this demand, publishing papers of high quality within the international state-of-the-art.

Therefore, ENIGMA – Brazilian Journal of Information Security and Cryptography – aims to fulfill this demand, and will publish state-of-art and original research papers and timely review articles on the theory, design, and evaluation of all aspects of information, network and system security.

II. ABOUT VOLUME 2, ISSUE 1 OF ENIGMA

In this issue of Volume 2 of ENIGMA – Brazilian Journal of Information Security and Cryptography – 6 papers are published. This section briefly presents the contribution of each of these papers.

The first selected paper, entitled "Proposal of Enhancement for Quartz Digital Signature", is published in Portuguese. In this paper, the authors propose a new digital signature scheme, based on the Quartz digital signature scheme, which pertains to the class of Hidden Field Equations (HFE), with a special choice of parameters. The presented scheme achieves an estimated security level estimated at 2^{112}, regarding adaptive chosen message attacks that make calls to the random Oracle.

The selected paper "Untappable Key Distribution System: a One-Time-Pad Booster", which is published in English, proposes a solution for the secure sharing and renewal of keys for the One-Time-Pad (OTP) protocol. To provide fast and unlimited renewal of secure keys, the proposed untappable key distribution system utilizes two layers of confidentially protection, based on the physical noise intrinsic to the optical channel and a bit pool of refreshed entropy.

Also in English, the selected paper "Cyber-Attacks Based in Electromagnetic Effects" covers cyber-attacks that take advantage of unintended electromagnetic emanations from the data sources, comprising a survey of some attacks, alongside with measurements that show the basic nature and underlying principles involved.

The first invited paper is "A Modularity and Extensibility Analysis on Authorization Frameworks", published in English, and presenting a comparative analysis between the existing authorization frameworks developed either within the academic and industry environments. This analysis uses a motivating example to present the main industry frameworks and consider the fulfillment of modularity, extensibility and granularity requirements facing its suitability for the existing access control models.

The next two invited papers come from relevant Brazilian conferences, being in this ENIGMA issue published in Portuguese. The first one, "The Producer-Consumer Collusion Attack in Content-Centric Networks", which was considered the 2nd best paper of SBRC´2015, evaluates the impact of a denial-of-service attack in information-centric networks based on the Content Centric Networking (CCN) architecture. In the considered attack, both malicious consumers and producers collude, by generating, publishing, and changing content popularity, thus increasing the content retrieval time.

Closing this ENIGMA issue, the invited paper "SpamBands - a Methodology to Identify Sources of Spam Acting in Concert", the best paper of SBSeg´2014, considers the relationships between the machines used to send spam as the basis for an analysis that could reveal how different machines may be used by a single spammer to spread his messages. Then, this work proposes a methodology to

E. T. Ueda, Institute for Technological Research of the State of São Paulo, edutakeo@usp.br

M. S. M. A. Notare, IEEE Latin America Transactions Editor in Chief, IEEE South Brazil, mirela@ieee.org

R. T. de Sousa Júnior, University of Brasilia, desousa@unb.br

cluster the machines used by spammers, thus identifying different aspects of the spam dissemination process.

III. CONCLUSION

ENIGMA – Brazilian Journal of Information Security and Cryptography – is now in its second year. Adopting since its creation the best practices from IEEE Transactions publications, it is hoped that soon this journal will become a reference among the leading international publication dedicated to information security and cryptography.

With the creation of this journal Brazil makes a considerable step toward the future, because the ENIGMA journal is an important tool for communication and integration of knowledge between universities, research centers, industries, government or military institutions around the world. Moreover, as threats to information security and privacy are risks for any nation, the ENIGMA journal can envision the international community.

ACKNOWLEDGEMENTS

We would like to thank all the authors who contributed with their papers for this issue of the ENIGMA journal, this publication would not exist if not for the dedication to their research. We must also thank all reviewers who worked very hard and in a timely fashion, so that we could select high quality papers. We are grateful to National Network of Information Security and Cryptography (RENASIC) and the Cyber Defense Center (CDCiber) of the Defense Minister of Brazil for their support in the creation of this journal, and the University of Brasilia (UnB) for providing space on one of their servers to host the official website of this journal. Moreover, we wish to thank Coronel Coronel Eduardo Wallier Vianna and Major Helder Vieira Bezerra for their support and in believing in this journal as well as their continuous help to get the printed version of this issue. Last but not least, thanks to Itamar Annoni Notare for his hard work and for his assistance in the revision process as well as on the formatting this journal.

Eduardo Takeo Ueda received the Ph.D. degree in Electrical Engineering in 2012, MSc degree in Computer Science in 2007, both from University of São Paulo (USP), and Specialist degree in Health Informatics in 2014 by Federal University of São Paulo (UNIFESP). He also holds a Mathematics degree by the São Paulo State University (UNESP), year 2000. His research interest includes topics of Cryptographic Algorithms and Protocols, Models of Access Control, and Computational Trust and Reputation. He has been committee member in conferences and reviewer of scientifics journals. Currently, he is Professor in Senac University Center of São Paulo, Master's Thesis Advisor in Institute for Technological Research of the State of São Paulo, member of the National Network of Information Security and Cryptography (RENASIC), and Editor in Chief of ENIGMA – Brazilian Journal of Information Security and Cryptography. http://lattes.cnpq.br/8367973725203446.

Mirela Sechi Moretti Annoni Notare received her Ph.D. and MSc degrees from the Federal University of Santa Catarina (UFSC) and a BSc degree from Passo Fundo University – all the three degrees in Computer Science. Her main research of interest focuses on the proposition of security management solutions for Wireless, Mobile, Sensor and Ad-Hoc Networks. Dra. Mirela Notare published widely in these areas. She also received several awards and citations, such as National Award for Telecommunication Software, British Library, TV Globo, INRIA and Elsevier Science. She served as General Co-chair for the I2TS (International Information and Telecommunication Technologies Symposium) and Program Co-Chair for the IEEE MobiWac (Mobility and Wireless Access Workshop) and IEEE ISCC. She has been a committee member in several scientific conferences, including ACM MSWiM, IEEE/ACM ANSS, IEEE ICC, IEEE IPDPS/WMAN IEEE/SBC SSI, and IEEE Globecom/Ad-Hoc, Sensor and Mesh Networking Symposium. She has been Guest Editor for several international journals, such as JOIN (The International Journal of Interconnection Networks), IJWMC (Journal of Wireless and Mobile Computing), JBCS (Journal of Brazilian Computer Society), Elsevier ScienceJPDC (The International Journal of Parallel and Distributed Computing), Wiley & Sons Journal of Wireless Communications & Mobile Computing, and Wiley InterScience Journal Concurrency & Computation: Practice & Experience. She has some Books and Chapters – Protocol Engineering with LOTOS/ISO (UFSC) and Solutions to Parallel and Distributed Computing Problems (Wiley Inter Science), for instance. She is the current Editor in Chief of IEEE Latin America Transactions magazine and Associate Editor in Chief of ENIGMA – Brazilian Journal of Information Security and Cryptography. She is the founding and president of STS Co, a senior member (21 years) of IEEE, and member of SBrT and SBC societies. http://lattes.cnpq.br/8224632340074096.

Rafael Timóteo de Sousa Júnior, was born in Campina Grande – PB, Brazil, on June 24, 1961. He graduated in Electrical Engineering, from the Federal University of Paraíba – UFPB, Campina Grande – PB, Brazil, 1984, and got his Doctorate Degree in Telecommunications, from the University of Rennes 1, Rennes, France, 1988. He worked as a software and network engineer in the private sector from 1989 to 1996. Since 1996, He is a Network Engineering Professor in the Electrical Engineering Department, at the University of Brasília, Brazil. From 2006 to 2007, supported by the Brazilian R&D Agency CNPq, He took a sabbatical year in the Group for the Security of Information Systems and Networks, at Ecole Superiéure d´Electricité, Rennes, France. He is a member of the Post-Graduate Program on Electrical Engineering (PPGEE) and supervises the Decision Technologies Laboratory (LATITUDE) of the University of Brasília. He is a member of the Brazilian Computer Society (SBC) and member of the National Network of Information Security and Cryptography (RENASIC). His field of study is distributed systems and network management and security. http://lattes.cnpq.br/3196088341529197.