ENIGMA – Brazilian Journal of Information Security and Cryptography

Call for Papers

Scope

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.

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.

In this manner, ENIGMA – Brazilian Journal of Information Security and Cryptography – will 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.

Important Dates

Submission deadline: 01 July 2012 (firm deadline)
Authors notification: 07 January 2013
Camera Ready version: 21 January 2013
Publishing: March 2013

Topics of Interest

Considering the goals presented above, ENIGMA – Brazilian Journal of Information Security and Cryptography – will publish original papers including (but not limited to) the following interest topics:

Authentication and Authorization
Anonymity and Privacy
Attacks on Information Systems
Attacks on Web Applications
Audit of Information Systems
Anti-Phishing, Anti-Spam, Anti-Fraud Techniques
Artificial Intelligence applied to Information Security
Biometrics in Security Systems
Combat Electronic Fraud
Computational Tools
Cryptographic Hash
Cryptographic Engineering
Cryptanalysis Methods
Critical Infrastructure Protection
Context-Based Security
Database Security
Digital Forensics
Efficient Implementation of Cryptographic Algorithms
Ethical and Legal Implications
Formal Methods for Security
Firewall Evasion Techniques
Game Theory in Information Security
Hacking and Cybercrimes
Honeypots and Honeynets
Hardware Security
Hardware for Information Security
High Performance Computing applied to Information Security
Intrusion Detection and Prevention
Incident Detection and Response
Intellectual Property Protection
Language-Based Security
Large-scale Attacks and Defense
Malware Detection and Analysis
Network Vulnerabilities
Organizational Security Policies
Public Key Cryptography
Public key infrastructure
Performance Security Solutions
Patents, Standards and Security Norms
Quantum Computing applied to Information Security
Quantum and Post-Quantum Cryptography
Modeling and Simulation of Security Systems
Software Vulnerabilities
Symmetric Cryptography
Secure Multi-Party Computation
Secure Software Development
Security Measures and Metrics
Security Risk Analysis
Security Protocols
Security in Operating Systems
Security in Service-Oriented Architecture
Security in Cloud Computing
Security in Mobile Communications
Trust Management and Reputation Systems
Validation, Verification, and Security Testing

Instructions for Authors
The papers must represent original contribution and cannot be, previous published (or in parallel submission) in any journals, magazines or conferences – printed or electronic.

The submissions can be written in Portuguese, Spanish or English; but, in any case, the title, the abstract and the keyword MUST be in English – since the best papers will be invited to submit extended version to be published at IEEE Latin America Transactions (Xplore, DOI, ISI http://thomsonreuters.com, Qualis). The submission must be in anonymous mode, without author names, affiliation, acknowledgement, or any other obvious reference to the authors. The paper size is from 8 to 12 pages long, and the detailed format instructions are available at http://www.ewh.ieee.org/reg/9/etrans/files/autor_revista_latin_america_v4.zip. All submissions shall be done via JEMS system, developed by SBC (Brazilian Computer Society) at https://submissoes.sbc.org.br/enigma. Late Submission shall not be accepted. For more information please contact journalenigma@gmail.com. The Journal’s website is still under construction.

Support

Defense Ministry / Brazilian Army / Department of Science and Technology / Center of Cyber Defense

Editor-in-Chief
Eduardo Takeo Ueda

Associate Editor-in-Chief
Mirela Sechi Moretti Annoni Notare