Lecture Notes in Computer Science 6480

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Marina L. Gavrilova   C.J. Kenneth Tan
Edward David Moreno (Eds.)

Transactions on Computational Science XI

Special Issue on Security in Computing, Part II

Springer

Editors-in-Chief

Marina L. Gavrilova
University of Calgary, Department of Computer Science
2500 University Drive N.W., Calgary, AB, T2N 1N4, Canada
E-mail: mgavrilo@ucalgary.ca

C.J. Kenneth Tan
Exascala Ltd.
Unit 9, 97 Rickman Drive, Birmingham B15 2AL, UK
E-mail: cjtan@exascala.com

Guest Editor

Edward David Moreno
DCOMP/UFS - Federal University of Sergipe
Aracaju/SE, Brazil
E-mail: edwdavid@gmail.com

Library of Congress Control Number: 2010939851

CR Subject Classification (1998): C.2, K.6.5, D.4.6, E.3, K.4.4, G.2

ISSN 0302-9743 (Lecture Notes in Computer Science)
ISSN 1866-4733 (Transaction on Computational Science)
ISBN-10 3-642-17696-8 Springer Berlin Heidelberg New York
ISBN-13 978-3-642-17696-8 Springer Berlin Heidelberg New York

springer.com

Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper 06/3180

LNCS Transactions on Computational Science

Computational science, an emerging and increasingly vital field, is now widely recognized as an integral part of scientific and technical investigations, affecting researchers and practitioners in areas ranging from aerospace and automotive research to biochemistry, electronics, geosciences, mathematics, and physics. Computer systems research and the exploitation of applied research naturally complement each other. The increased complexity of many challenges in computational science demands the use of supercomputing, parallel processing, sophisticated algorithms, and advanced system software and architecture. It is therefore invaluable to have input by systems research experts in applied computational science research.

Transactions on Computational Science focuses on original high-quality research in the realm of computational science in parallel and distributed environments, also encompassing the underlying theoretical foundations and the applications of large-scale computation. The journal offers practitioners and researchers the opportunity to share computational techniques and solutions in this area, to identify new issues, and to shape future directions for research, and it enables industrial users to apply leading-edge, large-scale, high-performance computational methods.

In addition to addressing various research and application issues, the journal aims to present material that is validated – crucial to the application and advancement of the research conducted in academic and industrial settings. In this spirit, the journal focuses on publications that present results and computational techniques that are verifiable.

Scope

The scope of the journal includes, but is not limited to, the following computational methods and applications:

- Aeronautics and Aerospace
- Astrophysics
- Bioinformatics
- Climate and Weather Modeling
- Communication and Data Networks
- Compilers and Operating Systems
- Computer Graphics
- Computational Biology
- Computational Chemistry
- Computational Finance and Econometrics
- Computational Fluid Dynamics

- Computational Geometry
- Computational Number Theory
- Computational Physics
- Data Storage and Information Retrieval
- Data Mining and Data Warehousing
- Grid Computing
- Hardware/Software Co-design
- High-Energy Physics
- High-Performance Computing
- Numerical and Scientific Computing
- Parallel and Distributed Computing
- Reconfigurable Hardware
- Scientific Visualization
- Supercomputing
- System-on-Chip Design and Engineering

Editorial

The Transactions on Computational Science journal is part of the Springer series *Lecture Notes in Computer Science*, and is devoted to the gamut of computational science issues, from theoretical aspects to application-dependent studies and the validation of emerging technologies.

The journal focuses on original high-quality research in the realm of computational science in parallel and distributed environments, encompassing the facilitating theoretical foundations and the applications of large-scale computations and massive data processing. Practitioners and researchers share computational techniques and solutions in the area, identify new issues, and shape future directions for research, as well as enable industrial users to apply the techniques presented.

The current volume is devoted to Security in Computing (Part 2), and is edited by Edward David Moreno. It is comprised of 14 selected papers that represent the diverse applications and designs being addressed today by the security and cryptographic research community. This special issue is devoted to state-of-the-art research on security in computing and includes a broad spectrum of applications such as new architectures, novel hardware implementations, cryptographic algorithms, and security protocols.

We would like to extend our sincere appreciation to Special Issue Guest Editor Edward David Moreno for his dedication and insights in preparing this high-quality special issue. We also would like to thank all authors for submitting their papers to the special issue, and to all associate editors and referees for their valuable work. We would like to express our gratitude to the LNCS editorial staff of Springer, in particular Alfred Hofmann, Ursula Barth, and Anna Kramer, who supported us at every stage of the project.

It is our hope that the fine collection of papers presented in this special issue will be a valuable resource for Transactions on Computational Science readers and will stimulate further research into the vibrant area of computational science applications.

October 2010

Marina L. Gavrilova
C.J. Kenneth Tan

Security in Computing:
Research and Perspectives, Part II
Special Issue Guest Editor's Preface

In an increasingly connected world, security has become an essential component of modern information systems. Our ever-increasing dependence on information implies that the importance of information security is growing. Several examples of security applications are present in everyday life such as mobile phone communication, internet banking, secure e-mail, data encryption, etc.

The thrust of embedded computing has both diversified and intensified in recent years as the focus on mobile computing, ubiquitous computing, and traditional embedded applications has begun to converge. A side effect of this intensity is the desire to support sophisticated applications such as speech recognition, visual feature recognition, and secure wireless networking in a mobile, battery-powered platform. Unfortunately these applications are currently intractable for the embedded space.

Another consideration is related to mobile computing, and, especially, security in these environments. The first step in developing new architectures and systems that can adequately support these applications is to obtain a precise understanding of the techniques and methods that come close to meeting the needs of security, performance, and energy requirements; with an emphasis on security aspects.

This special issue brings together high-quality and state-of-the-art contributions on security in computing. The papers included in this issue deal with some hot topics in the security research sphere: new architectures, novel hardware implementations, cryptographic algorithms and security protocols, and new tools and applications. Concretely, the special issue contains 14 selected papers that represent the diverse applications and designs being addressed today by the security and cryptographic research community.

As a whole, this special issue provides a vision on research and new perspectives in security research. With authors from around the world, these articles bring us an international sample of significant work.

The title of the first paper is "SEAODV: A Security Enhanced AODV Routing Protocol for Wireless Mesh Networks", by Celia Li, Zhuang Wang, and Cungang Yang. In this paper, the authors propose SEAODV, which is a security enhanced version of AODV (the Ad hoc On Demand Distance Vector). The AODV routing algorithm is a routing protocol designed for ad hoc mobile networks. The authors use Blom's key pre-distribution scheme to establish keys to ensure that every two nodes in the network uniquely share the pairwise keys. So, SEAODV adds secure AODV extensions to the original AODV routing messages, and it is lightweight and computationally efficient, since only symmetric cryptographic operations are involved. Finally, the authors carry out several tests and conclude that SEAODV offers superior performance in terms of computation cost and route acquisition latency as compares with two other secure routing protocols, ARAN and SAODV.

In the second contribution, which is entitled "Auto-Generation of Least Privileges Access Control Policies for Applications Supported by User Input Recognition", Sven Lachmund and Gregor Hengst present means to auto-generate least privileges access control policies for applications. The authors introduce and discuss two approaches: extending a static analysis approach by user input recognition, and introducing a new runtime approach on user input recognition that is based on information tracking and aspect-oriented programming. They show a third solution, combining the other two contributions with some of the existing work. A prototype in Java is implemented, and it is shown that the total number of aspects is kept within a manageable range, proving feasibility and scalability.

In the third contribution, which is entitled "Impossibility Results for RFID Privacy Notions", Frederik Armknecht, Ahmad-Reza Sadeghi, Alessandra Scafuro, Ivan Visconti, and Christian Wachsmann focus on the security and privacy model proposed by Paise and Vaudenay (PV-model) and investigate some subtle issues such as tag corruption aspects. The PV-model is one of the most comprehensive RFID security and privacy models up to date since it captures many aspects of real world RFID systems and aims at abstracting most previous works in a single concise framework. The authors point out subtle weaknesses and deficiencies in the PV-model.

In the fourth contribution, which is entitled "Implementation of Multivariate Quadratic Quasigroups for Wireless Sensor Networks", authored by Ricardo José Menezes Maia, Paulo Sérgio Licciardi Messeder Barreto, and Bruno Trevizan de Oliveira, a new approach to solving the problem of providing PKCs (public key cryptosystems) in WSNs (wireless sensor networks) is proposed. The authors use nesC and focus on modules for the encryption and decryption of a 160-bit MQQ (Multivariate Quadratic Quasigroup) algorithm that have been implemented on platforms TelosB and MICAz sensors.

In the fifth contribution, which is entitled "Hardware Architectures for Elliptic Curve Cryptoprocessors Using Polynomial and Gaussian Normal Basis Over GF(2^233)", by Vladimir Tujillo-Olaya and Jaime Velasco-Medina, the authors present two elliptic curve cryptoprocessors suitable for the computation of point multiplication over GF(2m) using Gaussian Normal Basis (GNB) and polynomial basis (PB). In this case, efficient hardware architectures are designed for finite field multiplication, in order to select the best implementation for the cryptoprocessor design. These multiplier architectures incorporate bit-serial and digit-serial algorithms. The authors designed cryptoprocessors using the same tools, FPGA, finite field *m* size and hardware description language, and show that the GNB cryptoprocessor presents a higher performance than the PB cryptoprocessor (but the scalability is an advantage of polynomial basis). So, they conclude that the designed cryptoprocessors present a high performance, use a small area, and provide a good time-area trade-off.

In the sixth paper "GPU Accelerated Cryptography as an OS Service", by Owen Harrison and John Waldron, the authors provide a standard method of access to the latest GPU crypto acceleration work to all components within an operating system, with minimal loss of performance. For this process, the authors have seen that the GPU can be effectively integrated into the OCF with careful design of a driver consisting of a kernelspace OCF driver and a userspace daemon. The results obtained show that there is an average overhead of 3.4% when using the OCF for AES over a standalone implementation. In the context of RSA-1024 we see that there is a very low 0.3% average overhead when compared with a standalone version.

In the seventh paper, which is entitled "From a Generic Framework for Expressing Integrity Properties to a Dynamic MAC Enforcement for Operating Systems", Patrice Clemente, Jonathan Rouzaud-Cornabas, and Christian Toinard propose a novel framework for expressing integrity requirements associated with direct or indirect activities, mostly in terms of information flows. The paper presents formalization for the major integrity security properties of the literature. The framework enables the user to formalize the major integrity security properties. The authors use a MAC enforcement mechanism implementing that algorithm to effectively and efficiently control those system calls.

In the eighth paper, which is entitled "Performance Issues on Integration of Security Services", Fábio Dacêncio Pereira and Edward David Moreno project and develop a SSIL (Security Services Integrated Layer) for allowing the integration of security services. They investigate the efficiency and impact of behavioral models used in SSIL specialized for detecting anomalies and conclude that there are advantages in having a set of security services in a single integrated system, since the possible fragility of a service can be compensated by others.

In the ninth paper "Statistical Model Applied to NetFlow for Network Intrusion Detection", André Proto, Leandro A. Alexandre, Maira L. Batista, Isabela L. Oliveira and Adriano M. Cansian present a proposal for event detection in computer networks using statistical methods and the analysis of NetFlow data flows. The aim is to use this proposal to monitor a computer network perimeter, detecting attacks in the shortest time possible through anomalies identification in traffic and alerting the administrator when necessary. The authors carry out a test for monitoring the system to four services widely used by users on the Internet: FTP, SSH, SMTP, and HTTP. Finally, the authors conclude that this methodology can be used for events detection in large-scale networks.

The paper "J-PAKE: Authenticated Key Exchange Without PKI", authored by Feng Hao and Peter Ryan, proposes a protocol called J-PAKE, which authenticates a password with zero-knowledge and then subsequently creates a strong session key if the password is correct. The authors show that the protocol fulfills some properties, and show how to effectively integrate the ZKP (Zero-Knowledge Proof) into the protocol design and achieve good efficiency. The authors have compared their approach with de facto internet standard SSL/TLS, and demonstrate that J-PAKE has comparable computational efficiency to the EKE and SPEKE schemes with clear advantages on security. For this reason it is more lightweight in password authentication.

The paper "Distance Based Transmission Power Control scheme for Indoor Wireless Sensor Networks", by P.T.V. Bhuvaneswari, V. Vaidehi, and M. Agnes Saranya, proposes a new scheme that is an energy efficient RSS (Received Signal Strength) based distributed localization algorithm and Distance Based Transmission Power Control (DBTPC). The proposed localization algorithm consists of two stages, namely, distance estimation and coordinates estimation, and with this it improves the accuracy in relative coordinate estimation and minimizes the energy cost incurred for transmitting information between nodes.

The paper "A Novel Feature Vectors Construction Approach for Face Recognition", by Paul Nicholl, Afandi Ahmad, and Abbes Amira, discusses a novel feature vectors construction approach for face recognition using DWT (Discrete Wavelet Transform). The authors evaluate the method using different classes of tests. The first set of experiments performed focused on the choice of DWT features. It is revealed that, where direct coefficient values were used for recognition, the LL quadrant provided the best results. The second set of tests were designed to identify which wavelet filters were the most effective at extracting features for face recognition with the specified database. Finally, the authors investigated two approaches, PMA and ORA, for the feature threshold, and their results show that the PMA is an ineffective approach, with recognition accuracy decreasing by an average of 0.025% from the results obtained without DWT coefficient selection.

The paper “An Extended Proof-Carrying Code Framework for Security Enforcement”, authored by Heidar Pirzadeh, Danny Dubé, and Abdelwahab Hamou-Lhadj, proposes a novel approach to solving the proof size problem while avoiding a significant increase of the TCB. The authors present an extension to a traditional proof-carrying code framework in which proofs tend to be too large to transmit. For this, their approach is based on the innovative idea of sending a program that generates the proof instead of the proof itself. Finally, they developed a virtual machine called the VEP (Virtual Machine for Extended PCC - Proof-Carrying Code) that runs on the consumer's side and that is responsible for running the proof generator program.

The last paper in this special issue, “NPT Based Video Watermarking with Non-overlapping Block Matching” by S.S. Bedi, Shekhar Verma, and Geetam S. Tomar, presents a NTP (Naturalness Preserving Transform) that is based on collusion and compression resistant watermarking techniques for video. Their experimental results confirm several theoretical findings and demonstrate the resistance of the technique to temporal frame averaging, additive noise, and JPEG based compression.

Finally, we sincerely hope that this special issue stimulates your interest in the many subjects surrounding the area of security. The topics covered in the papers are timely and important, and the authors have done an excellent job of presenting their different approaches. Regarding the reviewing process, our referees (integrated by recognized researchers from the international community) made a great effort to evaluate the papers. We would like to acknowledge their effort in providing us the excellent feedback at the right time. So, we wish to thank all the authors and reviewers. To conclude, we would also like to express our gratitude to the Editor-in-Chief of TCS, Dr. Marina L. Gavrilova, for her advice, vision, and support.

September 2010 Edward David Moreno

LNCS Transactions on Computational Science – Editorial Board

Table of Contents – Part II

Table of Contents – Part I