Lecture Notes in Computer Science 5430

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 IV

Special Issue on Security in Computing

Springer

Library of Congress Control Number: Applied for

CR Subject Classification (1998): D.4.6, C.2-4, F.2, E.1-4, K.4.4, K.6.5

ISSN	0302-9743 (Lecture Notes in Computer Science)
ISSN	1866-4733 (Transaction on Computational Science)
ISBN-10	3-642-01003-2 Springer Berlin Heidelberg New York
ISBN-13	978-3-642-01003-3 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12649952 06/3180 5 4 3 2 1 0

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

Security in Computing: Trends and Challenges

Guest Editor's Foreword

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, secure e-mail, internet banking, 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 which can adequately support these applications is a precise understanding of the techniques and methods that comes close to meeting the needs of security, performance, and energy requirements.

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 perspective on trends and challenges in security research. With authors from around the world, these articles bring us an international sampling of significant work.

The title of the first paper is "Hardware Mechanisms for Memory Authentication: A Survey of Existing Techniques and Engines," by Reouven Elbaz, David Champagne, Catherine Gebotys, Ruby B. Lee, Nachiketh Potlapally and Lionel Torres. This paper describes tree hardware mechanisms (Merkle Tree, PAT and TEC-Tree) that provide memory authentication and the architectural features proposed in the literature to efficiently implement those trees in computing platforms. The authors also discuss the impact of operating system compromise on the integrity verification engine and present an existing solution for secure and efficient application memory authentication despite an untrusted operating system. Finally, they show which additional security issues should be considered for data authentication at runtime in symmetric multi-processors platforms and how they differ from memory authentication in uniprocessor systems.

In the second contribution, entitled "Behavioral Characterization for Network Anomaly Detection," Victor P. Roche and Unai Arronategui propose a methodology for detecting abnormal traffic on the net, such as worm attacks, based on the observation of the behavior of different elements at the network edges. This methodology means an advance in the detection of a new infection in the backbone of the network, but also in the identification of the infected hosts of a specific network. The authors try to detect network anomalies by tracking the behavior of different network levels. This proposed method is not based on intrinsic characteristics of the worm but on their manner of acting. This methodology has proved its effectiveness in real infections caused by viruses such as SpyBot and Agobot in accordance with experimental tests.

In the third contribution, which is entitled "The Power of Anonymous Veto in Public Discussion," Feng Hao and Piotr Zielinski propose an exceptional solution—Anonymous Veto Network (or AV-net)—to allow a group of participants to compute a boolean-OR function securely. This protocol is provably secure under the Decision Diffie-Hellman (DDH) and random oracle assumptions. When compared with other related works, this solution does not require any private channels or third parties; it has no message collisions, hence requires no retransmissions; being semantically secure, it provides the strongest protection of a vetoer's anonymity until all the other participants are compromised; it resists robustly against jamming, hence ensures each participant's veto power; it requires only two rounds of broadcast. Finally, the computational load, the bandwidth usage, and the cost of verifying zero-knowledge proofs are also interesting.

The fourth contribution, which is entitled "Collusion-Resistant Message Authentication in Overlay Multicast Communication," by Emad Eldin Mohamed and Hussein Abdel-Wahab, introduces a new technique for collusion-resistant message authentication in overlay multicast. A basic feature of overlay multicast is that the receivers may also take over the responsibility of delivering the multicast traffic from the source to other group members. The proposed technique minimizes the computational cost through signature amortization. In order to evaluate their technique, the authors conducted a simulation study to compare the proposed technique against previous ones. Results obtained from the study show that the proposed technique is more suitable for overlay multicast than those developed for IP multicast. More specifically, the proposed technique has better communication and better receiver computation overheads (especially when forged messages are considered) than earlier ones.

In the fifth contribution, entitled "A Model for Authentication Credentials Translation in Service-Oriented Architecture," Emerson Ribeiro de Mello, Michelle S. Wangham, Joni da Silva Fraga, Edson T. de Camargo, and Davi da Silva Böger describe a model that enables authentication with SSO (single sign on), which was developed to simplify the interactions among clients and different service providers. This paper deals with interoperability between heterogeneous security technologies. The proposed model is based on the credential translation service that allows SSO, and even heterogeneous security technologies are considered. In the entire system, access authorizations to resources depend on this authentication, which sensibly diminishes the data flux between the domains and the management of these data in the system as a whole. Therefore, the proposed model provides authentication credential translation and attribute transposition and, as a consequence, provides authorization involving different kinds of credentials and permissions in the federation environment.

By making use of Web Services, this study is strongly based on concepts introduced in the SAML, WS-Trust, and WS-Federation specifications.

In the sixth paper, which is entitled "Secure and Efficient Group Key Agreements for Cluster Based Networks," Ratna Dutta and Tom Dowling consider that ad hoc networks may be logically represented as a set of clusters; they then present two dynamically efficient authenticated group key agreement protocols by reflecting ad hoc networks in a topology composed of a set of clusters. The protocols support dynamic membership events and their communication and computation efficiencies are favorably compared with a previous group of key agreement protocols in a cluster-based structure. The proposed protocols avoid the use of a trusted third party (TTP) or a central authority, eliminating a single point attack. They allow easy addition an removal of nodes, and achieve better performance in comparison with the existing cluster-based key agreement protocols. Additionally, their proposed schemes are supported by sound security analysis in formal security models under standard cryptographic assumptions. The authors have distinguished between the two approaches from a performance point of view and have shown that the second scheme is the better one in the context of wireless ad hoc networks.

In the seventh paper, entitled "An Integrated ECC-MAC Based on RS Code," Jaydeb Bhaumik and Dipanwita Roy Chowdhury propose a new integrated scheme for message authentication (MAC algorithm) based on RS code having t-symbol error correcting capability. In their proposed MAC generation algorithm, the authors used a function Nmix for mixing the sequence with the error-correcting check symbols. The proposed scheme is secured even if the same pad is used for more than one MAC generation. The proposed function reduces the bias of linear approximations exponentially. In addition, the proposed MAC is found to be a good choice for the keyed-hash technique and evaluated successfully for bit-variance and entropy test. The proposed function can be used effectively as a key mixing function in hardware-based block ciphers.

In the eighth paper, which is entitled "Optimizing Pseudonym Updation in Vehicular Ad-hoc Network," Brijesh Kumar Chaurasia, Shekhar Verma, G. S. Tomar, and Ajith Abraham focus on the problem of diminishing the possibility of forging a relationship between vehicle identity and its transmissions by determining the conditions that maximize anonymity during an identity switch. A vehicle can be tracked through its transmission. The broadcast by a source contains its current identity and also allows estimation of its location by receivers. This mapping between the physical entity and the estimated location through the communication broadcast is a threat to privacy. Therefore, this paper addresses the challenges in providing anonymity to a moving vehicle that uses a temporary identity for transmission and continually changes this pseudonym. The authors propose a heuristic that allows a vehicle to switch its pseudonym at a time and place where the anonymity can be maximized. Results indicate that updating pseudonyms in accordance with the heuristic maximizes the entropy and, through it, the anonymity of a vehicle.

The paper "Security Analysis of Role-Based Access Control Models Using Colored Petri Nets and CPNtools" authored by Hind Rakkay and Hanifa Boucheneb presents a formal technique to model and analyze role based access control models (RBAC) using colored Petri nets (CP-nets) and CPN-tools for editing and analyzing CP-nets

which describes generic access control structures based on an RBAC policy that can then be composed with different context-specific aspects depending on the application. In this way, RBAC aspects can be reused across different applications with similar access control requirements. The authors propose an analysis framework that can be used by security administrators to generate correct specification iteratively. A significant benefit of CP-nets and, particularly, CPN-tools is to provide a more intuitive way for system developers to model and analyze complex systems.

The paper "Role-Based Access Control with Spatiotemporal Context for Mobile Applications," by Subhendu Aich, Samrat Mondal, Shamik Sural, and Arun Kumar Majumder, proposes a complete RBAC model in a spatiotemporal domain based on the idea of spatiotemporal extent. The concept of a spatiotemporal role extent and spatiotemporal permission extent introduced here enables the model to specify granular spatiotemporal access control policies not specifiable in the existing approaches. In a typical access request, a user activates a suitable role where the required permission to access the requested object is available. Thus in classical RBAC, role and permission are important logical entities through which a user ultimately gains the access to an object. The concept of spatiotemporal access is introduced in the form of role extent, and permission extent, which is simple to understand and expressive in terms of specifying combined space time-based security policy. As a proof of concept, the authors have implemented the proposed spatiotemporal access control method in a mobile telemedicine system.

The paper "A Method for Estimation of the Success Probability of an Intrusion Process by Considering the Time Aspects of the Attacker Behavior" authored by Jaafar Almasizadeh and Mohammad Abdollahi Azgomi proposes a generic and new method for modeling and quantifying the security of computer systems. The authors utilize stochastic modeling techniques for quantitative assessment of security measures for computer systems. In the proposed method, intrusion process is divided into its principal phases. At each phase, the probability of attacker success is computed. It is assumed that the attacker will finally succeed if he can pass all steps successfully. The interaction between the attacker and the system is displayed by a semi-Markov chain (SMC). Intrusion process modeling is done by an SMC. Distribution functions assigned to SMC transitions are uniform distributions. Uniform distributions represent the sojourn time of the attacker or the system in the transient states. This probability is a numerical measure for the security level provided by the system. Then the SMC is converted into a discrete-time Markov chain (DTMC). The DTMC is analyzed and the probability of attacker success is then computed based on mathematical theorems. Thus the security measure can be obtained.

The paper "A Hardware Architecture for Integrated-Security Services," authored by Fabio Dacêncio Pereira and Edward David Moreno, proposes a special architecture and describes the functionalities of an embedded system of SSI (integration of the security services), which prevents malicious attacks on systems and networks. It was implemented in an embedded security system (into a SoC system). The different modules dedicated to security such as AES, RSA, HASH, among others, were implemented. It is important to note that the performance statistics (runtime related to circuit delays) and physical area of implementation in hardware are presented and discussed. It reaches an improved performance and the SoC prioritizes the implementation of dedicated functions

in hardware such as cryptographic algorithms, communication interfaces, among others. In their prototype, initially, the flow control functions and settings are running in software. This article shows the architecture, functionality, and performance of the system developed, and the authors discuss a real implementation in FPGA.

The paper "Evaluating Resistance of MCML Technology to Power Analysis Attacks Using a Simulation-Based Methodology" authored by Francesco Regazzoni et al. presents a simulation-based methodology for evaluating the resistance of cryptographic circuits to power analysis attacks. The authors used a special methodology to evaluate the MCML technology as a possible counter-measure against side channel attacks based on power analysis, and demonstrated the robustness of MCML against the SPA and against the powerful variant of DPA based on correlation. To achieve this result, they developed a design flow and a SPICE-level simulation environment. Their results show that the power traces obtained by simulating two full cores, implementing the AES algorithm and realized in MCML, are very difficult to attack, as opposed to an CMOS implementation for which the same attacks were always successful.

The last paper in this special issue, "Putting Trojans on the Horns of a Dilemma: Redundancy for Information Theft Detection" by Jedidiah R. Crandall, John Brevik, Shaozhi Ye, Gary Wassermann, Daniela A.S. de Oliveira, Zhendong Su, S. Felix Wu, and Frederic T. Wong, presents an approach that detects information theft by measuring explicitly everything that could have happened. The authors propose a technique based on repeated deterministic replays in a virtual machine to detect the theft of private information. The authors prove upper bounds on the average amount of information an attacker can steal without being detected, even if they are allowed an arbitrary distribution of visible output states.

To conclude, we sincerely hope that this special issue stimulates your interest in the many issues 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 researches from the international community) made a great effort to evaluate the papers. We would like to acknowledge their effort in providing us with the excellent feedback at the right time. Therfore, we wish to thank all the authors and reviewers. Finally, we would also like to express our gratitude to the Editor-in-Chief of TCS, Marina L. Gravilova, for her advice, vision and support.

January 2009 Edward David Moreno

LNCS Transactions on Computational Science – Editorial Board

Reviewers

Ayda Saidane	University of Trento, Italy
Azzedine Benameur	SAP Research, Security & Trust
Babak Salamat	University of California, Irvine
Barbara Catania	University of Genoa, Italy
Billy Brumley	Helsinki University of Technology, Finland
Brian Rogers	North Carolina State University, USA
Brijesh Kumar Chaurasia	Indian Institute of Information Technology, Allahabad, India
Byeong Ho Kang	School of Computing and ISs, Univeristy of Tasmania, Australia
Carlos Maurício Seródio Figueiredo	FUCAPI – Analysis, Research and Technological Innovation Center, Brazil
Changda Wang	Jiangsu University, China
Christian Damsgaard Jensen	Informatics & Mathematical Modelling, Technical University of Denmark
Conghua Zhou	Jiangsu University, China
David Champagne	Princeton University, USA
Denivaldo Lopes	Federal University of Maranhão, Brazil
E. Munivel	DOEACC – Calicut, India
Eduardo F. Nakamura	FUCAPI – Analysis, Research and Technological Innovation Center, Brazil
Edward David Moreno	UEA – University of Amazonas State, Manaus, Brazil
Emad Eldin Mohamed	College of IT, United Arab Emirates University, UAE
Feng Hao	Thales Information Systems Security, UK
Francesco Regazzoni	USI – ALaRI, Lugano, Switzerland
Guilherme Ottoni	Intel Research Labs
Gunes Kayacik	Dalhousie University, Canada
Hind Rakkay	École Polytechnique de Montréal, Canada
Hirofumi Sakane	National Institute of Advanced Industrial Science and Technology (AIST), Japan
Hoon Ko	GECAD, ISEP, IPP, Portugal
Jaafar Almasizadeh	Iran University of Science and Technology, Iran
Jaime Velasco Medina	University of Valle, Cali, Colombia
Jason D. Hiser	University of Virginia, USA
Jedidiah Crandall	University of New Mexico, Dept. of Computer Science, USA
Jeong Ok Kwon	Korea University, Korea
Jonathan Katz	University of Maryland, USA
Junho Lee	Korea University, Korea

Konstantinou Elisavet	Department of Information and Communication Systems Engineering, University of the Aegean, Samos, Greece
Leonardo Augusto Ribeiro	University of Pernambuco, UFPE, Brazil
Luiza de Macedo Mourelle	State University of Rio de Janeiro, Brazil
Maria Luisa Damiani	University of Milan, Italy
Martin Drahansky	Brno University of Technology, Faculty of Information Technology, Czech Republic
Martin Rehak	Czech Technical University in Prague, Czech Republic
Mehran Misaghi	SOCIESC (Sociedade Educacional de Santa Catarina), Brazil
Meuse Nogueira de Oliveira Júnior	Federal Center of Technological Education of Pernambuco State, Brazil
Michael Kirkpatrick	Purdue University, USA
Michelle Silva Wangham	University of Vale do Itajaí (UNIVALI), Brazil
Mikaël Ates	Université de Lyon – University Jean Monnet of Saint-Etienne
Milena Milenkovic	IBM
Mohsen Toorani	Iran University of Science and Technology, Iran
Nachiketh Potlapally	Intel Corporation
Nadia Nedjah	State University of Rio de Janeiro, Brazil
Naixue Xiong	Department of Computer Science, Georgia State University, USA
Neil Vachharajani	Google
Nur Zincir-Heywood	Dalhousie University, Canada
Paolo Perlasca	University of Milan, Italy
Phongsak Keeratiwintakorn	King Mongkut's University of Technology North Bangkok, Thailand
Raimundo da Silva Barreto	Federal Universitiy of Amazonas, Brazil
Rami Yared	JAIST – Japan Advanced Institute of Science and Technology, Japan
Ratna Dutta	Claude Shannon Institute, NUIM, Maynooth, Ireland
Ren-Chiun Wang	Department of Electrical Engineering, National Taiwan University, Taiwan
Reouven Elbaz	University of Waterloo, Canada
Ruy de Queiroz	University of Pernambuco, UFPE, Brazil
Shamik Sural	School of Information Technology, Indian Institute of Technology, India
Siddhartha Chhabra	NC State University, USA
Steven Galbraith	Mathematics Department at Auckland University, New Zealand
Tai-hoon Kim	Hannam University, Korea
Tamás Holczer	BME, Budapest, Hungary

Víctor Pérez-Roche	University of Zaragoza, Spain
Wassim El-Hajj	College of Information Technology, UAE University, UAE
Woo Kwon Koo	CIST, Korea
Yan Solihin	NC State University, USA
Yang Xiang	Central Queensland University, Australia
Yeu-Pong Lai	Department of Computer Science and Information Engineering, Chung Cheng Institute of Technology, National Defence University, China
Yingpeng Sang	School of Computer Science at University of Adelaide, Australia

Table of Contents