J Supercomput (2011) 55: 1–3
DOI 10.1007/s11227-009-0361-y

Guest editorial: high performance trusted computing

Keqiu Li · Hai Jin · Jingwei Jin

Published online: 27 November 2009

Nowadays, information security has become a key challenge for designers and developers of most systems and applications. Under the situation, TC (trusted computing) is required. In technical fields, US government issued TCSEC (trusted computer system evaluation criteria) in 1983. The Trusted Computing Group (TCG), successor to the Trusted Computing Platform Alliance (TCPA), is an initiative started by AMD, Hewlett-Packard, IBM, Infineon, Intel, Microsoft, and Sun in 2003. In research fields, IEEE has published the transactions on dependable and secure computing in 2004. With the development of trusted computing application, trusted computing technology has become a hot topic in the field of information security. To provide snapshots of current research in the field of high performance trusted computing, we map out this special issue to document state-of-the-art research, new developments, and directions for future investigation in this field. This special issue consists of six papers, selected from twenty-one submitted papers, which can be considered a significant contribution to the field of high performance trusted computing. We expect that our selection could provide the usual readers of the journal with useful knowledge. We

K. Li (✉)
Department of Computer Science and Engineering, Dalian University of Technology, No 2, Linggong Road, Dalian 116024, China
e-mail: keqiu@dlut.edu.cn

H. Jin
School of Computer Science and Technology, Huazhong University of Science and Technology, Wuhan 430074, China
e-mail: hjin@hust.edu.cn

J. Jin
School of Management, Dalian University of Technology, No 2, Linggong Road, Dalian 116024, China
e-mail: jinyw@dlut.edu.cn

also wish that this special issue could attract more readers to the journal. This special issue is organized as follows.

The first paper, "*Embedded Access Points for Trusted Data and Resources Access in HPC Systems*," authored by C. Militello et al., presents hardware access point for HPC environments. The access point is composed of a fingerprint scanner, a smartcard reader, and a hardware core for fingerprint processing and matching. Experimental trials conducted on several fingerprint DBs show that hardware prototype achieves a working point with FAR = 1.07% and FRR = 8.33% on a proprietary DB acquired via a capacitive scanner, a working point with FAR = 0.66% and FRR = 6.13% on a proprietary DB acquired via an optical scanner, and a working point with FAR = 1.52% and FRR = 9.64% on the official FVC2002 DB2B database. In the best-case scenario (depending on fingerprint image size), the execution time of the proposed recognizer is 183.32 ms.

The second paper, "*Leakage-efficient Design of Value Predictors through State and Non-state Preserving Techniques*," authored by Juan M. Cebrián et al., proposes a leakage-efficient design of traditional Value Predictors (VP) based on the fact that many VP entries remain unused during long periods of time before being eventually evicted. By applying both state and non-state preserving techniques, the unused entries are disabled obtaining substantial leakage energy reductions (50–80%, depending on the configuration and predictor type).

The third paper, "*Automatically Constructing Trusted Cluster Computing Environment*," authored by Yongwei Wu et al., proposes a methodology of Trusted Cluster Computing (TCC) to automatically construct user-trustable cluster computing environment. User-specified applications are downloaded from user-specified location and automatically and dynamically deployed on cluster nodes. To reduce the overhead of this dynamic deployment, a novel Heuristics-based Overhead-Reducing (HOR) replacement strategy is also proposed. A highly configurable simulator has been implemented to perform a series of simulations. The simulation results show that the HOR can produce an Average Speedup with up to 14% (light workload), 8% (heavy workload) and 10% (medium workload) higher than that of LRU-based strategies, with a typical setting of ARDE being 0.2.

In the paper "*Building an Automated Trust Negotiation Architecture in Virtual Computing Environment*," Deqing Zou et al. propose an automated trusted negotiation architecture which the authors call the virtual automated trust negotiation (VATN) to centralize ATN policies and credentials for multiple virtual machines into a privileged virtual machine. VATN puts policy compliance checker and credential verification control in each virtual machine to improve the execution efficiency of trust negotiation. The authors implemented VATN in Xen virtualization platform and discuss the correctness of policy consistency checking and make performance analysis of VATN implemented in Xen.

The fifth paper, "*Reliable Network-on-Chip Design for Multi-Core System-on-Chip*," authored by Kuei-chung Chang et al., presents a simple coding scheme for reducing power dissipation, crosstalk noise, and crosstalk delay on the bus, while simultaneously detecting errors at runtime. It uses a simple bus-invert encoding technique to reduce the prohibited transitions in terms of crosstalk noise and power dissipation. The authors also design a corresponding detector to detect errors at the input

of the NoC routers. It can save energy by interrupting communications without storing and routing the packets when errors occur during transmissions. The experimental results for various multimedia applications show significant reduction in the number of patterns that are most likely to produce crosstalk errors. The results also show that it is attractive in terms of cost to apply the detecting logic to routers in the NoC with respect to the power consumption.

The reliability and scalability of large-scale network storage systems are confronted with the big challenge. It is necessary to design a reliable, scalable, and efficient data placement algorithm. The last paper in this special issue, "*Reliable, Scalable and Efficient Data Placement Algorithm*," authored by Nong Xiao, Tao Chen, Fang Liu, describes RSEDP, combined of RRDP (reliable replication data placement) and SEDP (scalable and efficient data placement), to achieve the above-mentioned design requirements. Both the theoretical analysis and the experimental study show that the combined RSEDP can increase redundancy degree and failure resilience, has good scalability and time-efficiency with a little memory overhead.

The guest editors want to express their gratitude to all the reviewers for their qualified and expedite help in evaluating the submitted papers. We also want to thank Editor-in-Chief, Prof. Hamid R. Arabnia, who gave his full support in this special issue.