Guest Editors' Introduction: Special Issue on Trust, Security, and Privacy in Parallel and Distributed Systems

Zhenfu Cao, *Senior Member, IEEE*, Keqiu Li, *Senior Member, IEEE*, Xu Li,
Patrick McDaniel, *Senior Member, IEEE*, Radha Poovendran, *Senior Member, IEEE*,
Guojun Wang, *Member, IEEE*, and Yang Xiang, *Senior Member, IEEE*

✦

IN modern computing paradigms, most computing systems, e.g., cluster computing, grid computing, cloud computing, the Internet, telecommunication networks, Cyber-Physical Systems (CPS), and Machine-to-Machine communication networks (M2M), are parallel and distributed systems. While providing improved expandability, manageability, efficiency, and reliability, parallel and distributed systems increase their security weaknesses to an unprecedented scale. As the system devices are widely connected, their vulnerabilities are shared by the entire system. Because tasks are allocated to, and information is exchanged among the system devices that may belong to different users, trust, security, and privacy issues have yet to be resolved. This special issue of the *IEEE Transactions on Parallel and Distributed Systems* (*TPDS*) highlights recent advances in trust, security, and privacy for emerging parallel and distributed systems.

This special issue was initiated by Dr. Xu Li, Dr. Patrick McDaniel, Dr. Radha Poovendran, and Dr. Guojun Wang. Due to a large number of submissions, Dr. Zhenfu Cao, Dr. Keqiu Li, and Dr. Yang Xiang were later invited to the editorial team. Dr. Xu Li was responsible for coordinating the paper review process. In response to the call for papers, we received 150 effective submissions, out of which 24 are included in this special issue after rigorous review and careful revision, presenting an acceptance ratio of 16 percent. The accepted papers are divided into three groups, covering issues related to trust, security, and privacy, respectively.

- Z. Cao is with the Department of Computer Science, Shanghai Jiao Tong University (SJTU), 800 Dongchuan Rd, Shanghai 200240, China. E-mail: zfcao@cs.sjtu.edu.cn.
- K. Li is with the School of Computer Science and Technology, Dalian University of Technology, No 2, Linggong Road, Dalian 116023, China. E-mail: keqiu@dlut.edu.cn.
- X. Li is with Huawei Technologies Canada, Suite 400, 303 Terry Fox Dr., Ottawa, ON, Canada K2K 3J1. E-mail: easylix@gmail.com
- P. McDaniel is with the Department of Computer Science and Engineering, College of Engineering, Pennsylvania State University, 360A Information Sciences and Technology Building, University Park, PA 16802-6823. E-mail: mcdaniel@cse.psu.edu.
- R. Poovendran is with the Electrical Engineering Department, University of Washington, Box 352500, Paul Allen Building, Seattle, WA 98195-2500. E-mail: RP3@UW.EDU.
- G. Wang is with the School of Information Science and Engineering, Central South University, Computer Building 406-B, Changsha, Hunan Province 410083, P.R. China. E-mail: csgjwang@gmail.com.
- Y. Xiang is with the School of Information Technology, Deakin University, 221 Burwood Highway, Burwood, VIC 3125, Australia. E-mail: yang@deakin.edu.au

For information on obtaining reprints of this article, please send e-mail to: tpds@computer.org.

The first group includes five papers on trust issues.

The paper "Verifying Keys through Publicity and Communities of Trust: Quantifying Off-Axis Corroboration" proposes to achieve robust verification with a novel theoretical model, called Public Data, which treats operational deployments as communities of trust and makes them the verification substrate.

The paper "Trustworthy Operations in Cellular Networks: The Case of PF Scheduler" proposes a trustworthy version of the proportional fair scheduler for cellular networks to mitigate the effects of DoS attacks, where malicious UEs disrupt service by intelligently faking their CQI and ARQ feedback reports.

The paper "Traffic Pattern-Based Content Leakage Detection for Trusted Content Delivery Networks" addresses content leakage during video streaming and proposes a content-leakage detection scheme that is robust to the variation of video length by exploiting the relation between video length and content similarity.

The paper "Enabling Trustworthy Service Evaluation in Service-Oriented Mobile Social Networks" proposes a trustworthy service evaluation system to enable service review sharing in mobile social networks. It identifies three service review attacks and develops sophisticated security mechanisms to deal with these attacks.

The paper "ReDS: A Framework for Reputation-Enhanced DHTs" presents a framework for enhancing lookups in redundant Distributed Hash Table (DHTs) in peer-to-peer network by tracking how well nodes service lookup requests and study the collaborative identification and removal of bad lookup paths in a way that does not rely on the sharing of reputation score.

The second group contains six papers addressing privacy issues.

The paper "Certificateless Remote Anonymous Authentication Schemes for Wireless Body Area Networks" presents a pair of light-weight authentication protocols, based on an efficient and secure certificateless signature scheme, to enable remote wireless body area network users to anonymously enjoy healthcare service.

The paper "LocaWard: A Security and Privacy Aware Location-Based Rewarding System" proposes a location-based rewarding system for location-based services, where mobile users can collect and redeem location-based tokens for beneficial rewards. A security and privacy aware rewarding protocol is developed for the system, along with correctness and completeness proofs.

The paper "Internet Traffic Privacy Enhancement with Masking: Optimization and Trade-Offs" studies if and how complex it is to mask traffic, i.e., to obfuscate information leaked by packet traffic features, namely, packet lengths, directions, and times. It defines an optimized traffic masking algorithm that removes any leaking and investigates the trade-off between privacy protection and masking cost.

The paper "A Scalable Two-Phase Top-Down Specialization Approach for Data Anonymization Using MapReduce on Cloud" proposes a scalable two-phase approach to anonymize large-scale data sets using the MapReduce framework on cloud. In both phases, a group of innovative MapReduce jobs are designed to concretely accomplish the specialization computation in a highly scalable way.

The paper "Exploiting Service Similarity for Privacy in Location-Based Search Queries" proposes a user-centric location-based service architecture where a user can observe the impact of location inaccuracy on the service accuracy before deciding the geo-coordinates to use in a query.

The paper "Decentralized Access Control with Anonymous Authentication for Securing Data in Clouds" proposes a distributed privacy preserving authenticated access control scheme for securing data in clouds. In the scheme, the cloud verifies user authenticity before storing information, without knowing user ID, and only valid users are able to decrypt stored information.

The last and largest group deals with security problems and contains 13 papers.

The paper "RRE: A Game-Theoretic Intrusion Response and Recovery Engine" proposes an approach enabling automated response in the face of fast-spreading intrusions. The approach employs a game-theoretic response strategy against adversaries modeled as opponents in a two-player Stackelberg stochastic game.

The paper "Enabling Data Integrity Protection in Regenerating-Coding-Based Cloud Storage: Theory and Implementation" studies the problem of remotely checking the integrity of regenerating-coded data against corruptions under a real-life cloud storage setting. A solution is designed and implemented for a specific regenerating code.

The paper "Balancing Performance, Accuracy, and Precision for Secure Cloud Transactions" addresses the risk of having inconsistent authorization policies or user credentials in distributed database systems over cloud servers. It proposes several increasingly stringent policy consistency constraints and different enforcement approaches.

The paper "Dynamic Authentication with Sensory Information for the Access Control Systems" introduces an authentication technique by combining the sensory information from onboard sensors on access cards and the original encoded identification information. It tackles problems such as access card loss, stolen and duplication.

The paper "Distributed, Concurrent, and Independent Access to Encrypted Cloud Databases" proposes a novel architecture that integrates cloud database services with data confidentiality and the possibility of executing concurrent and independent operations on encrypted data.

The paper "A System for Denial-of-Service Attack Detection Based on Multivariate Correlation Analysis" presents a DoS attack detection system, which extracts the geometrical correlations between network traffic features, characterizes traffic Multivariate Correlation Analysis, and applies anomaly-based detection principle.

The paper "A UCONabcResilient Authorization Evaluation for Cloud Computing" provides resilience to UCONabc continuous authorization reevaluation, by dealing with individual exception conditions, such as disparity among usage accounting and authorization attributes, while maintaining a suitable access control.

The paper "Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage" shows how to securely, efficiently, and flexibly share data in cloud storage and describes new public-key cryptosystems which produce constant-size ciphertexts such that efficient delegation of decryption rights for any set of ciphertexts are possible.

The paper "A Distributed Information Divergence Estimation over Data Streams" investigates how to detect and quantify the amount of work performed by an adversary over data streams and proposes a novel algorithm for estimating the Kullback-Leibler divergence of an observed stream compared to the expected one.

The paper "FLAP: An Efficient WLAN Initial Access Authentication Protocol" points out that the authentication inefficiency of IEEE 802.11 under some scenarios is a framework design issue—too many messages are introduced —and propose an access authentication protocol using less messages along with security proof.

The paper "Collaborative Policy Administration" tackles the privilege overclaim issue in policy management by a novel policy administration mechanism, in which a policy administrator can refer to other similar policies to set up their own policies to protect privacy and other sensitive information.

The paper "An Error Minimizing Framework for Localizing Jammers in Wireless Networks" presents a framework that can localize one or multiple jammers with a high accuracy in wireless communications. It employs an estimation scheme based on ambient noise floor and validates it through real-world experiments.

The paper "Securing Broker-Less Publish/Subscribe Systems Using Identity-Based Encryption" presents a novel approach to providing confidentiality and authentication in a broker-less content-based publish-subscribe system. The approach provides fine-grained key management, and its associated cost for encryption, decryption and routing is in the order of subscribed attributes.

Zhenfu Cao
Keqiu Li
Xu Li
Patrick McDaniel
Radha Poovendran
Guojun Wang
Yang Xiang
Guest Editors
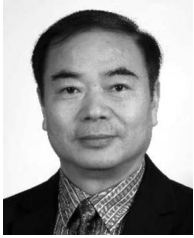
Zhenfu Cao received the BSc degree in computer science and technology and the PhD degree in mathematics from the Harbin Institute of Technology, Harbin, China, in 1983 and 1999, respectively. His research interests mainly include number theory, cryptography, and information security. Since 1981, he has published more than 400 academic papers in journals or conferences. He has directed more than 50 research projects at national or provincial levels. He is currently a distinguished professor and the director of the Trusted Digital Technology Laboratory, Shanghai Jiao Tong University, Shanghai, China. He also serves as a member of the expert panel of the National Nature Science Fund of China. He is actively involved in the academic community, serving as committee/cochair, program committee member, and/or associate editor for several international conferences and journals. He has received a number of awards, including the Youth Research Fund Award of the Chinese Academy of Science in 1986, the Ying-Tung Fok Young Teacher Award in 1989, the National Outstanding Youth Fund of China in 2002, the Special Allowance by the State Council in 2005, and a corecipient of the 2007 IEEE International Conference on Communications-Computer and Communications Security Symposium Best Paper Award in 2007. Professor Cao is also the leader of the Asia 3 Foresight Program (61161140320) and the key project (61033014) of National Natural Science Foundation of China. He is a senior member of the IEEE.
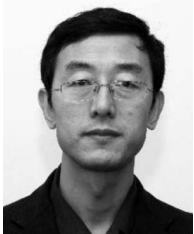
Keqiu Li is currently a professor in the School of Computer Science and Technology, Dalian University of Technology, China. He received the bachelor's and master's degrees, both from Dalian University of Technology, China, in 1994 and 1997, and the doctorate degree from the Japan Advanced Institute of Science and Technology in 2005. He was a research fellow at the University of Tokyo, Japan, from October 2005 to September 2007. He also has five years of experience in industry. His research interests include content distribution network, cloud computing, data center network, and wireless computing. He has published more than 100 technical papers in international journals and conferences. He is on the committee board for several international/national journals including *TPDS* and *TC*, and serves as organization chair/program chair/publication chair/program committee member for a couple of international conferences. He received best paper awards at HPCC 2012, ICA3PP 2011, and ICCNMC 2005. He is a senior member of the IEEE.
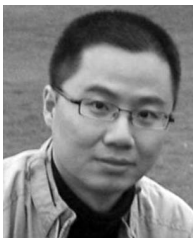
Xu Li is a research engineer at Huawei Technologies Canada. Prior to joining Huawei, he worked at Inria, France, as a research scientist. He received the PhD (2008) degree from Carleton University, the MSc (2005) degree from the University of Ottawa, and the BSc (1998) degree from Jilin University, China, all in computer science. His current research interests are focused in next-generation wireless networks, along with more than 70 refereed publications. He is/was on the editorial boards of *TPDS*, the *Wiley Transactions on Emerging Telecommunications Technologies, Ad Hoc & Sensor Wireless Networks*, and *Parallel and Distributed Computing and Networks*. He is TPC cochair of GC '13 Ad Hoc and Sensor Networking Symposium. He was a recipient of NSERC PDF awards and a number of other awards.

Patrick McDaniel is a professor in the Computer Science and Engineering Department at the Pennsylvania State University and co-director of the Systems and Internet Infrastructure Security Laboratory. His research efforts centrally focus on network, telecommunications, and systems security, language-based security, and technical public policy. Professor McDaniel has published more than 150 papers, articles, and reports on a broad range of security and networking topics. He has chaired several top conferences including, among others, the 2007 and 2008 IEEE Symposium on Security and Privacy and the 2005 USENIX Security Symposium. Prior to pursuing the PhD degree in 1996 at the University of Michigan, he was a software architect and project manager in the telecommunications industry. Professor McDaniel assumed the chair position of the IEEE Computer Society Technical Committee on Security and Privacy in January 2014. He is a senior member of the IEEE.

Radha Poovendran is a professor and founding director of the Network Security Lab (NSL) in the Electrical Engineering (EE) Department at the University of Washington (UW). He is a founding member and the associate director of research of the University of Washington Center for Excellence in Information Assurance Research and Education. His research interests are in the areas of wireless and sensor network security, adversarial modeling, privacy and anonymity in public wireless networks, control-security, games-security and Information Theoretic-Security in the context of wireless mobile networks. Professor Poovendran is a recipient of the NSA LUCITE Rising Star Award (1999), US National Science Foundation CAREER (2001), US ARO YIP (2002), US ONR YIP (2004), and PECASE (2005) for his research contributions to multi-user wireless security. He is also a recipient of the Outstanding Teaching Award and Outstanding Research Advisor Award from UW EE (2002) and Graduate Mentor Award from Office of the Chancellor at the University of California San Diego (2006). He was coauthor of award-winning papers including IEEE&IFIP William C. Carter Award Paper (2010) and WiOpt Best Paper Award (2012). He has cochaired multiple conferences and workshops including the first ACM Conference on Wireless Network Security (WiSec) in 2008 and the NITRD-NSF National workshop on high-confidence transportation cyber-physical systems in 2009, trustworthy aviation information systems at the 2010 and 2011 AIAA Infotech@Aerospace and 2011 IEEE Aerospace. He was chief editor for the *Proceedings of the IEEE* special issue on cyber-physical systems (2012), an editor of *TMC* and *ACM TOSN*, coguest editor for two special issues on security and privacy (*IEEE Networks* 2013; *IEEE TPDS* 2013). He cochairs IEEE CNS 2014. He is a senior member of the IEEE.

Guojun Wang received the BSc degree in geophysics, the MSc degree in computer science, and the PhD degree in computer science, at Central South University, China, in 1992, 1996, 2002, respectively. He is currently the Chairman, Professor, and Doctoral Supervisor of Department of Computer Science at CSU. He is also the Director of Trusted Computing Institute at CSU. He has been an Adjunct Professor at Temple University, USA; a Visiting Scholar at Florida Atlantic University, USA; a Visiting Researcher at the University of Aizu, Japan; and a Research Fellow at the Hong Kong Polytechnic University, HK. His research interests include trusted computing, information security, transparent computing/Cloud computing. He has published more than 180 technical papers and books/chapters in the above areas. He is an associate editor or on editorial board of some international journals including *TPDS*, *Security and Communication Networks* (*SCN*), *International Journal of Parallel, Emergent and Distributed Systems* (*IJPEDS*), and *International Journal of Computational Science and Engineering* (*IJCSE*). He is the Leading Founder of the IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom). He is a member of IEEE (2010-), a member of ACM (2011-), a member of IEICE (2011-), a senior member of CCF (2005-), an executive member of the Council of Hunan Provincial Association of Computers (2011-), and a vice chairman of the Changsha Section of CCF (2013-).

Yang Xiang received the PhD degree in computer science from Deakin University, Australia. He is currently a full professor in the School of Information Technology, Deakin University. He is the Director of the Network Security and Computing Lab (NSCLab). His research interests include network and system security, distributed systems, and networking. He has served as the Program/General Chair for many international conferences such as ICA3PP 12/11, IEEE/IFIP EUC 11, IEEE TrustCom 13/11, IEEE HPCC 10/09, IEEE ICPADS 08, NSS 11/10/09/08/07. He has been the PC member for more than 60 international conferences in distributed systems, networking, and security. He serves as an associate editor of *TC*, *TPDS*, *Security and Communication Networks* (Wiley), and the editor of *Journal of Network and Computer Applications*. He is the Coordinator, Asia for the IEEE Computer Society Technical Committee on Distributed Processing (TCDP). He is a senior member of the IEEE.