Guest Editorial
Special Issue on Security for IoT: The State of the Art

THE INTERNET is becoming more and more ubiquitous. One central element of this trend is the existence of a massive network of interconnected wired/wireless physical objects, things, sensors, and devices, which can interact in a rich set of manners through a worldwide communication and information infrastructure to provide value added services. The vision of such an Internet of Things (IoT) system, supported by industrial companies and governments globally, has the potential to mark an evolution that will surely have a great impact on our environment and our lives.

Yet, the realization of a ubiquitous IoT also poses a number of challenges where security is among the top concerns. The globally interconnected physical objects inevitably result in a potentially enormous attack surface that can be easily exploited if not adequately protected. To enable strong security foundations for the ubiquitous IoT, many factors need to be taken into account. Examples are data security, privacy, access control, information assurance, trust management, secure services interoperability, seamless integration, system heterogeneity, scalability, and mobility. This Special Issue brings together the most recent advances in IoT security. The accepted papers pertain to the state-of-the-art security and privacy issues with respect to various pervasive and ubiquitous scenarios.

Out of 30 submissions received in response to the Calls for Papers of the Special Issue, seven papers have been accepted. The list and a brief summary of these papers are reported below.

We hope that readers will find the issue interesting and a source of inspiration for their future research and practical development work.

PAPERS

"Sybil Attacks and Their Defenses in the Internet of Things," by Kuan Zhang Xiaohui Liang, Rongxing Lu, and Sherman Shen, studies different types Sybil attacks in IoT and presents a suite of security solutions.

"Security Protocols and Privacy Issues into 6LoWPAN Stack: A Synthesis," by Christine Hennebert and Jessye Dos Santos, presents the benefits and limitations of a number of protocols and security solutions that can be deployed with constrained resources in IoT.

"Characterizing the Performance of Security Functions in Mobile Computing Systems," by Abdulmonem Rashwan, Abd-Elhamid Taha, and Hossam Hassanein, proposes a benchmarking environment for evaluating cryptography-based security functions from a communication perspective.

"P3: Privacy Preservation Protocol for Automatic Appliance Control Application in Smart Grid," by Depeng Li, Zeyar Aung, John Williams, and Abel Sanchez, investigates possible sensitive information leakages and analyzes potential privacy threats in the automatic appliance control application for IoT.

"Privacy Preserving Channel Access for Internet of Things," by Debasmit Banerjee, Bo Dong, Mahmoud Taghizadeh, and Subir Biswas, presents a privacy-aware slotted channel access mechanism for IoT in a multi-trust-domain environment.

"A Model-Based Validated Autonomic Approach to Self-Protect Computing Systems," by Qian Chen, Sherif Abdelwahed, and Abdelkarim Erradi, introduces an autonomic model-based cyber security management approach for the IoT ecosystems.

"An Anti-Tracking Source-Location Privacy Protection Protocol in WSNs Based on Path Extension," by Wei Tan, Ke Xu, and Dan Wang, proposes a new Path Extension Method scheme that provides strong protection for source location privacy in WSNs.

KUI REN
Computer Science and Engineering Department
State University of New York at Buffalo
Buffalo, NY 14260 USA

PIERANGELA SAMARATI
Department of Computer Science
Università degli Studi di Milano
Milan 26013, Italy

MARCO GRUTESER
Electrical and Computer Engineering Department
Rutgers University
New Brunswick, NJ 08901 USA

PENG NING
Department of Computer Science
North Carolina State University
Raleigh, NC 27695 USA

YUNHAO LIU
School of Software Engineering
Tsinghua University
Beijing 100084, China

Digital Object Identifier 10.1109/JIOT.2014.2361608

Kui Ren (A'07–M'07–SM'11) received the B.E. and M.E. degrees from Zhejiang University, Hangzhou, China, and the Ph.D. degree from Worcester Polytechnic Institute, Worcester, MA, USA.

Currently, he is an Associate Professor with the Computer Science and Engineering Department, State University of New York at Buffalo, Buffalo, NY, USA. His research interests include cloud computing security, wireless security, and IoT security. His research has been supported by the NSF, DoE, AFRL, Amazon, and MSR.

Dr. Ren serves as an Associate Editor for the IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, IEEE WIRELESS COMMUNICATIONS, the IEEE INTERNET OF THINGS JOURNAL, and the IEEE TRANSACTIONS ON SMART GRID, among others. He is a member of the ACM, a Distinguished Lecturer of the IEEE Vehicular Technology Society, and a past board member of the Internet Privacy Task Force, State of Illinois. He was a recipient of the NSF CAREER Award in 2011 and Sigma Xi/IIT Faculty Research Award in 2012. He was also the recipient of the Best Paper Award from IEEE ICNP 2011.

Pierangela Samarati (M'97–SM'10–F'12) is a Professor with the Department of Computer Science, Università degli Studi di Milano, Milan, Italy. She has been a Computer Scientist with the Computer Science Laboratory, SRI, Menlo Park, CA, USA. She has been a Visiting Researcher with the Computer Science Department, Stanford University, Stanford, CA, USA, and at the Center for Secure Information System, George Mason University, Fairfax, VA, USA. Her research interests include data security and privacy; access control policies, models, and systems; information system security; and information protection in general. She has participated in several projects involving different aspects of information protection. On these topics she has authored or coauthored more than 240 papers in international journals, conference proceedings, and book chapters.

Prof. Samarati is the Chair of the IEEE Systems Council Technical Committee on Security and Privacy in Complex Information Systems (TCSPCIS) and of the Steering Committees of the European Symposium on Research in Computer Security (ESORICS) and of the ACM Workshop on Privacy in the Electronic Society (WPES). She is a member of several Steering Committees. She was an ACM Distinguished Scientist in 2009. She was the recipient of the IFIP TC11 Kristian Beckman Award in 2008 and the IFIP WG 11.3 Outstanding Research Contributions Award in 2012.

Marco Gruteser (A'12) received the M.S. and Ph.D. degrees from the University of Colorado, Boulder, CO, USA, in 2000 and 2004, respectively.

He is an Associate Professor of electrical and computer engineering with Rutgers University, New Brunswick, NJ, USA. He is a member of the Wireless Information Network Laboratory (WINLAB). He has held research and visiting positions at the IBM T. J. Watson Research Center and Carnegie Mellon University. His research interests include location privacy and connected vehicles. Beyond these topics, his more than 100 peer-reviewed papers and patents span a wide range of wireless, mobile systems, and pervasive computing issues. His work has been regularly featured in the media, including NPR, the New York Times, Fox News TV, and CNN TV.

Dr. Gruteser has served as program Co-Chair or Vice-Chair for conferences such as ACM MobiSys, ACM WiSec, IEEE VNC, and IEEE Percom. He has delivered six conference and workshop keynotes, served as panel moderator at ACM MobiCom, and as panelist at ACM MobiSys, IEEE Infocom, and IEEE ICC. He was elected Treasurer and member of the Executive Committee of ACM SIGMOBILE. He was the recipient of an NSF CAREER Award, a Rutgers Board of Trustees Research Fellowship for Scholarly Excellence, a Rutgers Outstanding Engineering Faculty Award, as well as Best Paper Awards at ACM MobiCom 2012, ACM MobiCom 2011, and ACM MobiSys 2010.

Peng Ning (M'00–SM'12) received the B.S. degree in information sciences and M.E. degree in communications and electronics systems from the University of Science and Technology of China (USTC), Hefei, China, in 1994 and 1997, respectively, and the Ph.D. degree in information technology from George Mason University, Fairfax, VA, USA, in 2001.

He is a Professor of computer science with North Carolina State University, Raleigh, NC, USA, where he also serves as the Technical Director for Secure Open Systems Initiative (SOSI). His research has been supported by the NSF, Army Research Office (ARO), the Advanced Research and Development Activity (ARDA), IBM Research, SRI International, and the NCSU/Duke Center for Advanced Computing and Communication (CACC).

Dr. Ning is currently the Secretary/Treasurer of the ACM Special Interest Group on Security, Auditing, and Control (SIGSAC) and is on the Executive Committee of ACM SIGSAC. He is an Editor for Springer Briefs in Computer Science, responsible for briefs on information security. He has served or is serving on the Editorial Boards of several international journals, including the *ACM Transactions on Sensor Networks*, *Journal of Computer Security*, *Ad-Hoc Networks*, *Ad-Hoc and Sensor Networks: An International Journal*, *International Journal of Security and Networks*, and *IET Proceedings Information Security*. He also served as the Program Chair or Co-Chair for ACM SASN'05, ICICS'06, ESORICS'09, ICDCS-SPCC'10, and NDSS'13, the General Chair of ACM CCS'07 and '08, and Program Vice Chair for ICDCS'09 and ICDCS'10—Security and Privacy Track. He served on the Steering Committee of ACM CCS from 2007 to 2011 and is a founding Steering Committee member of ACM WiSec and ICDCS SPCC. He is a senior member of the ACM, and ACM SIGSAC. He was a recipient of the National Science Foundation (NSF) CAREER Award in 2005.

Yunhao Liu (S'03–M'04–SM'06) received the B.S. degree in automation from Tsinghua University, Beijing, China, in 1995, and the M.S. and Ph.D. degrees in computer science and engineering from Michigan State University, East Lansing, MI, USA, in 2003 and 2004, respectively.

He is currently the Chang Jiang Professor with the School of Software and TNLIST, Tsinghua University. His research interests include wireless sensor network, peer-to-peer computing, and pervasive computing.