Information Systems Frontiers

ISF Website

CALL FOR PAPERS

Special Issue on

Science of Cyber Security

Cyber attacks impose huge threats on digitally enabled organizations. To adequately manage cybersecurity risk and protect information assets, we must understand the capabilities and limitations of both cyber attacks and defenses. The unpleasant state-of-the-art is that cyber defense and management remains mostly heuristic and qualitative, and is viewed largely as an art rather than a science. The importance and urgency of elevating the art of cyber security to the envisioned science of cyber security is well recognized, as justified by the emergence of venues such as the International Conference on Science of Cyber Security (SciSec) in 2018.

This special issue will invite some of the papers that are presented at, and appear in the Proceedings of, the 2nd International Conference on Science of Cyber Security (SciSec'2019), which will be held August 9-11, 2019 in Nanjing, China. In line with the mission of the conference, this special issue aims to catalyze research collaborations between the relevant communities and disciplines to deepen our understanding of, and build a firm foundation for, the emerging Science of Cyber Security. Publications in this venue would distinguish themselves by taking or thinking from a holistic perspective about cyber security, rather than a building-blocks perspective.

Since the Proceedings of SciSec'2019 will be published as a volume in Springer's Lecture Notes in Computer Science, each invited paper will be requested to substantially extend its Proceedings version by introducing (30% or more) new materials. Each submission will be reviewed by at least 3 reviewers.

Submission Instruction

Manuscripts must be submitted in PDF format to the ISF-Springer online submission system at http://www.editorialmanager.com/isfi/ and the authors need to select "Special Issue: Science of Cyber Security" during the submission process. Paper submissions must conform to the format guidelines of Information Systems Frontiers available at http://www.springer.com/business/business+information+systems/journal/10796. Submissions should be approximately 32 pages double spaced including references.

Topics of interest include, but are not limited to:

- Cybersecurity Dynamics
- Cybersecurity Metrics and Their Measurements
- First-principle Cybersecurity Modeling and Analysis (e.g., Dynamical Systems, Control-Theoretic, and Game-Theoretic Modeling)
- Cybersecurity Data Analytics
- Quantitative Risk Management for Cybersecurity
- Big Data for Cybersecurity
- Artificial Intelligence for Cybersecurity
- Machine Learning for Cybersecurity
- Economics Approaches for Cybersecurity
- Social and Organizational Approaches for Cybersecurity
- Statistical Physics Approaches for Cybersecurity
- Complexity Sciences Approaches for Cybersecurity
- Experimental Cybersecurity
- Macroscopic Cybersecurity
- Statistics Approaches for Cybersecurity
- Human Factors and User Behaviors for Cybersecurity
- Compositional Security
- Biology-inspired Approaches for Cybersecurity
- Synergetics Approaches for Cybersecurity

Important Dates

Paper submission deadline: November 5, 2019
Notification of first round reviews: January 15, 2020
Revised manuscripts due: February 20, 2020
Notification of second round reviews: March 20, 2020
Final Version Due: April 20, 2020

Guest Editors

Jingguo Wang, University of Texas at Arlington, USA
Shouhuai Xu, University of Texas at San Antonio, USA
Moti Yung, Google and Columbia University, USA

Guest Editors' Biography

Jingguo Wang is a Professor of Information Systems, College of Business, University of Texas at Arlington (UTA). He earned his Ph.D. from University at Buffalo, State University of New York. His work has been published in the leading journals of Information Systems including MIS Quarterly, Information Systems Research, Journal of Management Information Systems, and Journal of the Association for Information Systems. His current research interests focus on information security, mostly investigating security behaviors of end users and risk management practices of organizations. He has been serving as a guest associate editor of MIS Quarterly, and an associate editor of MIS Quarterly Special Issue on Information Systems Security in a Digital Economy. He is currently serving as a coordinating editor of Information Systems Frontier, an associate editor of Decision Support Systems, and on the editorial board of Journal of Database Management. He also served as an associate editor of ICIS track in Security and Privacy, a review coordinator of WITS, and a program co-chair of Dewald Roode Workshop (IFIP WG8.11/WG11.13). He has been on the Program Committees of a number of international

conferences/workshops, and a reviewer for various journals. His research has been supported by National Science Foundation and the University of Texas at Arlington.

Shouhuai Xu is a Full Professor in the Department of Computer Science, University of Texas at San Antonio (UTSA). He is the founding director of the Laboratory for Cybersecurity Dynamics (LCD). His research expertise is in Cybersecurity, including theoretical cybersecurity foundation, quantitative cybersecurity management and operations, and practical cybersecurity architectures and mechanisms. He has served as an Associate Editor for IEEE Transactions on Information Forensics and Security (IEEE T-IFS) and for IEEE Transactions on Dependable and Secure Computing (IEEE TDSC) and is serving as an Associate Editor for IEEE Transactions on Network Science and Engineering (IEEE TNSE). He is/was a Program Committee co-chair of SciSec'2019, SciSec'2018, NSS'15 and Inscrypt'13. He co-initiated the new conference SciSec (*International Conference on Science of Cyber Security*) in 2018. He has served on the Program Committees of numerous international conferences/workshops. He has pioneered the systematically approach of Cybersecurity Dynamics, which aims to quantify and manage cybersecurity and cyber defense operations from a holistic perspective. This approach is inherently multidisciplinary and interdisciplinary, leading to publications across disciplines (including ACM Transactions, IEEE Transactions, Journal of Computer Security, Internet Mathematics, Technometrics, Journal of Applied Statistics, and Physical Review E). He received a PhD degree in Computer Science from Fudan University. His website is at www.cs.utsa.edu/~shxu.

Moti Yung is a Security and Privacy Scientist with Google, with main interests in Cryptography, Security, and Privacy. He graduated from Columbia University in 1988 and is an adjunct senior research faculty at Columbia till today. In parallel to Columbia he has had an industrial research career, working at places like IBM, RSA Labs. (EMC), Snap, and now Google. Yung is a fellow of ACM, of IEEE, of the International Association for Cryptologic Research (IACR) and the European Association for Theoretical Computer Science (EATCS). Among his awards are ACM's SIGSAC Outstanding Innovation Award in 2014, and 2018 IEEE Computer Society W. Wallace McDowell Award. His research covers broad areas: from the theory and foundations, to applied systems, and actual engineering efforts of cryptography, privacy, and secure systems. http://www.cs.columbia.edu/~moti/.