Xinming (Simon) Ou

Curriculum Vitae

Computer Science and Engineering
University of South Florida
4202 East Fowler Avenue, ENB 118
Tampa, FL 33620-5399

Office: (813)-974-4522
FAX: (813) 974-5456
xou@usf.edu
http://www.cse.usf.edu/~xou/

Education

- **Princeton University**, PhD., 2005, Computer Science
- **Tsinghua University**, M. E., 2000, Computer Science
- **Tsinghua University**, B. E., 1998, Computer Science

Appointments

- **University of South Florida**,
  Associate Professor, Aug 2015 – present,
- **Kansas State University**,
  Peggy and Gary Edwards Chair in Engineering, July 2014 – Aug 2015
  Associate Professor, July 2012 – Aug 2015, Assistant Professor, Aug 2006 – June 2012.
- **Idaho National Laboratory**, Research Associate, May 2006 – Aug 2006.
- **Purdue University**, Post-doc, Sept 2005 – May 2006.
- **HP Labs – Princeton**, Summer Intern, June 2005 – Sept 2005.
- **Microsoft Research – Redmond**, Summer Intern, June 2004 – Aug 2004.
- **Compaq/HP Systems Research Center (SRC)**, Summer Intern, June 2002 – Aug 2002.

Awards

- National Science Foundation Faculty Early Career Development (CAREER) Award. 2010.
- HP Labs Innovation Research Program (IRP) Award. 2010, 2011, 2012.
- K-State College of Engineering Frankenhoff Outstanding Research Award. 2013.

Grants

1. SaTC: CORE: Small: Collaborative: Data-driven Approaches for Large-scale Security Analysis of Mobile Applications (PI). National Science Foundation. $200,000, 8/15/2017-8/14/2020.
2. Developing Full Spectrum Cybersecurity Intelligence/Analytic Capabilities for the U.S. Army Reserve (co-PI). National Security Agency. $760,349, 9/16/2016 - 9/15/2017.
3. CRISP Type 2: Integrative Decision Making Framework to Enhance the Resiliency of Interdependent Critical Infrastructures (co-PI). National Science Foundation. $1,963,542, 9/1/2016 - 8/31/2020.
4. Modeling Security/Safety Interactions in Buildings for Compositional Security/Safety Control (PI). Department of Homeland Security CPSSEC program. $914,353, 10/1/2015-9/30/2018. (*Contract awarded to Kansas State after I moved to USF, but I am still responsible for the overall project.*)
5. MRI: Acquisition of an Adaptive Data Cluster for Data-intensive Applications in Science and Engineering (co-PI). National Science Foundation. $300,000, 9/1/2014-08/31/2017.

6. Enhancing the Cybersecurity and Information Assurance Research and Education Infrastructure at Kansas State University (PI). Defense University Research Instrumentation Program (DURIP), Air Force Office of Scientific Research (AFOSR). $605,650, 9/30/2013-9/29/2014.
7. TWC SBE TTP: Medium: Bringing Anthropology into Cybersecurity (PI). National Science Foundation. $715,845, 9/1/2013-8/31/2017.
8. Building the National Cyber Workforce: New SFS Program at Kansas State University (PI). National Science Foundation. $2,370,436, 1/1/2013-12/31/2017.
9. Techniques for Security Risk Analysis and Mitigation for Enterprise Networks (PI). National Institute of Standards and Technology, Measurement Science and Engineering (MSE) Research Grant Programs. $30,000, 8/1/2012-5/31/2013.
10. Understanding and Quantifying the Impact of Moving Target Defenses on Computer Networks (co-PI). Air Force Office of Scientific Research. $1,000,311, 4/1/2012-9/30/2017.
11. An Innovative Cybersecurity Curriculum for Civilian and Military Workforce (PI). National Science Foundation, Scholarship for Service (SFS) program. $299,652, 9/15/2011-9/14/2014.
12. Components, Run-time Substrates, and Systems: Medium: Holonic Multi-Agent Control of Intelligent Power Distribution Systems (co-PI). National Science Foundation, Cyber-Physical Systems (CPS) program. $1,100,000, 9/1/2011-8/31/2014.
13. Cyber-security partnership between Kansas State University and CABEM/NTS (co-PI). National Technical Systems. $98,000, 02/01/2011-01/31/2012.
14. TC:Small:Collaborative Research:Models and Techniques for Enterprise Network Security Metrics (PI). National Science Foundation. $396,676, 10/1/2010-9/30/2014.
15. A New Approach to Rigorous Risk Analytics using Attack Graphs (PI). HP Labs Innovation Research Program. $220,716, 8/1/2010-7/31/2013.
16. CAREER: Reasoning under Uncertainty in Cybersecurity (PI). National Science Foundation. $457,373, 3/1/2010 - 2/28/2017.
17. Evidence-based Trust in Large-Scale MLS Systems (co-PI). Air Force Office of Scientific Research. $3,000,000, 3/1/2009 - 11/30/2014.
18. CT-ISG: Model-Based, Automatic Network Security Management (PI). National Science Foundation. $245,000+$13,500 REU, 8/1/2007 - 7/31/2010.
19. A Domain Specific Language for Defining High-Assurance Secure Network Guards (co-PI). Rockwell Collins, Inc. $170,000, 9/22/2008 - 8/31/2009.
20. Automatic Control-Network Security Management Using Attack Graphs (PI). Department of Energy (through Idaho National Laboratory). $35,000, 3/20/2007 - 8/17/2007.

Publications

1. Yuping Li, Jiyong Jang, Xin Hu, and Xinming Ou. Android malware clustering through malicious payload mining. In *the 20th International Symposium on Research on Attacks, Intrusions and Defenses (RAID 2017)*, Atlanta, GA, September 18-20, 2017. (Acceptance rate: 20%)
2. Alexandru G. Bardas, Sathya C. Sundaramurthy, Xinming Ou and Scott A. Deloach. MTD CBITS: Moving target defense for cloud-based IT systems. In *22nd European Symposium on Research in Computer Security (ESORICS'17)*, Oslo, Norway, September 11-13, 2017. (Acceptance rate: 16%)
3. Fengguo Wei, Yuping Li, Sankardas Roy, Xinming Ou, and Wu Zhou. Deep ground truth analysis of current Android malware. In *14th Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA 2017)*, Bonn, Germany. July 6-7, 2017. (Acceptance rate: 27%)
4. Xiaolong Wang, Richard Habeeb, Xinming Ou, Siddharth Amaravadi, John Hatcliff, Masaaki Mizuno, Mitchell Neilsen, S. Raj Rajagopalan, Srivatsan Varadarajan. Enhanced security of building automation systems through microkernel-based controller platforms. In *The Second IEEE In-*

ternational Workshop on Communication, Computing, and Networking in Cyber Physical Systems (CCNCPS 2017), Atlanta, GA, USA, June 5, 2017.

5. Sathya Chandran Sundaramurthy, Michael Wesch, Xinming Ou, John McHugh, S. Raj Rajagopalan, and Alexandru G. Bardas. Humans are dynamic – our tools should be too. *IEEE Internet Computing*, Volume: 21, Issue: 3, May-June 2017.
6. Jaime C. Acosta, Edgar Padilla, John Homer, and Xinming Ou. Risk analysis with execution-based model generation. *Journal of Cyber Security and Information Systems*, Vol 5, No. 1, December, 2016.
7. Jordan DeLoach, Doina Caragea, and Xinming Ou. Android malware detection with weak ground truth data. In *3rd International Workshop on Pattern Mining and Application of Big Data (BigPMA)*, Washington D.C., USA, December 5-8, 2016.
8. Xinming Ou. A bottom-up approach to applying graphical models in security analysis (invited paper). In *Third International Workshop on Graphical Models for Security (GraMSec)*, Lisbon, Portugal, June 27, 2016. Lecture Notes in Computer Science, Vol 9987, pp 1-24, September, 2016.
9. Sathya Chandran Sundaramurthy, John McHugh, Xinming Ou, Michael Wesch, Alexandru G. Bardas, and S. Raj Rajagopalan. Turning contradictions into innovations or: How we learned to stop whining and improve security operations. In *Symposium On Usable Privacy and Security (SOUPS 2016)*, Denver, CO, USA, June 22-24, 2016. (Acceptance rate: 28%)
10. Sankardas Roy, Jordan DeLoach, Yuping Li, Nic Herndon, Doina Caragea, Xinming Ou, Venkatesh Prasad Ranganath, Hongmin Li, and Nicolais Guevara. Experimental study with real-world data for Android app security analysis using machine learning. *31st Annual Computer Security Applications Conference (ACSAC)*, Los Angeles, California, USA, Dec 7-11, 2015. (Acceptance rate: 24%)
11. Su Zhang, Xinming Ou, and Doina Caragea. Predicting cyber risks through National Vulnerability Database. *Information Security Journal: A Global Perspective* 24:4-6, 194-206, Taylor & Francis, Nov 30, 2015.
12. Su Zhang, Xinwen Zhang, Xinming Ou, Nigel Edwards, Jing Jin, and Liqun Chen. Assessing attack surface with component-based package dependency. In *the 9th International Conference on Network and System Security* (NSS), New York, USA, November, 2015. (Acceptance rate: 36%)
13. Xiaolong Wang, Masaaki Mizuno, Mitch Neilsen, Xinming Ou, S. Raj Rajagopalan, Will G. Baldwin, and Bryan Phillips. Secure RTOS architecture for building automation. In *First ACM Workshop on Cyber-Physical Systems Security and Privacy (CPS-SPC)*, Denver, CO, USA, October, 2015.
14. Rui Zhuang, Alexandru G. Bardas, Scott A. Deloach, and Xinming Ou. A theory of cyber attacks – a step towards analyzing MTD systems. In *CCS 2015 MTD Workshop*, Denver, CO, USA, October, 2015.
15. Stefan Nagy, Imani Palmer, Sathya Chandran Sundaramurthy, Xinming Ou, and Roy Campbell. An empirical study on current models for reasoning about digital evidence. In *10th International Conference on Systematic Approaches to Digital Forensic Engineering (SADFE)*, Málaga, Spain, Sept 30-Oct 2, 2015.
16. Yuping Li, Sathya Chandran Sundaramurthy, Alexandru G. Bardas, Xinming Ou, Doina Caragea, Xin Hu, and Jiyong Jang. Experimental study of fuzzy hashing in malware clustering analysis. In *8th Workshop on Cyber Security Experimentation and Test (CSET'15)*, Washington, D.C., USA, Aug 10, 2015. (Acceptance rate: 31%)
17. Sathya Chandran Sundaramurthy, Alexandru G. Bardas, Jacob Case, Xinming Ou, Michael Wesch, John McHugh, and S. Raj Rajagopalan. A human capital model for mitigating security analyst burnout. In *Symposium On Usable Privacy and Security (SOUPS 2015)*, Ottawa, Canada, July 22-24, 2015. (**Distinguished Paper Award**. Acceptance rate: 25%)
18. Justin Paupore, Earlence Fernandes, Atul Prakash, Sankardas Roy, and Xinming Ou. Practical always-on taint tracking on mobile devices. In *15th Workshop on Hot Topics in Operating Systems (HotOS'15)*, Kartause, Switzerland, May 18-20, 2015. (Acceptance rate: 32%)

19. Hussain M.J. Almohri, Layne T. Watson, Danfeng Yao, and Xinming Ou. Security optimization of dynamic networks with probabilistic graph modeling and linear programming. *IEEE Transactions on Dependable and Secure Computing (TDSC)*, vol.PP, no.99, March 2015.
20. Ian Unruh, Alexandru G. Bardas, Rui Zhuang, Xinming Ou, and Scott A. DeLoach. Compiling abstract specifications into concrete systems - bringing order to the cloud. In *28th Large Installation System Administration Conference (LISA'14)*, Seattle, WA, USA, Nov, 2014. (Acceptance rate: 27%)
21. Fengguo Wei, Sankardas Roy, Xinming Ou, and Robby. Amandroid: A precise and general inter-component data flow analysis framework for security vetting of Android apps. In *ACM Conference on Computer and Communications Security (CCS 2014)*, Scottsdale, AZ, USA, Nov, 2014. (Acceptance rate: 20%)
22. Rui Zhuang, Scott A. DeLoach, and Xinming Ou. Towards a theory of moving target defense. In *The First ACM Workshop on Moving Target Defense (MTD 2014)*, Scottsdale, AZ, USA, Nov, 2014.
23. Sathya Chandran Sundaramurthy, John McHugh, Xinming Ou, S. Raj Rajagopalan, and Michael Wesch. An anthropological approach to studying CSIRTs. *IEEE Security & Privacy*, Volume: 12, Issue: 5, Special Issue on CSIRTs, Sept/Oct, 2014.
24. Su Zhang, Xinwen Zhang, and Xinming Ou. After we knew it: Empirical study and modeling of cost-effectiveness of exploiting prevalent known vulnerabilities across IaaS cloud. In *9th ACM Symposium on Information, Computer and Communications Security (ASIACCS)*, Kyoto, Japan, June, 2014. (Acceptance rate: 15%)
25. Rui Zhuang, Scott A. DeLoach, and Xinming Ou. A model for analyzing the effect of moving target defenses on enterprise networks. In *9th Cyber and Information Security Research Conference (CSIRC)*, Oak Ridge, Tennessee, USA, April, 2014.
26. Scott DeLoach, Xinming Ou, Rui Zhuang, and Su Zhang. Model-driven, moving-target defense for enterprise network security. In *Uwe Aβmann, Nelly Bencomo, Gordon Blair, Betty H. C. Cheng, Robert France (eds) State-of-the-Art Survey Volume on Models @run.time*. Springer LNCS, 2014.
27. Loai Zomlot, Sathya Chandran Sundaramurthy, Doina Caragea, and Xinming Ou. Aiding intrusion analysis using machine learning. *12th International Conference on Machine Learning and Applications (ICMLA)*, Miami, Florida, USA, December, 2013. (Acceptance rate: 26%)
28. John Homer, Su Zhang, Xinming Ou, David Schmidt, Yanhui Du, S. Raj Rajagopalan, and Anoop Singhal. Aggregating vulnerability metrics in enterprise networks using attack graphs. *Journal of Computer Security*, Vol 21, No 4., September, 2013.
29. Rui Zhuang, Su Zhang, Alexandru G. Bardas, Scott A. DeLoach, Xinming Ou, and Anoop Singhal. Investigating the application of moving target defenses to network security. *6th International Symposium on Resilient Control Systems (ISRCS)*, San Francisco, CA, USA, August, 2013.
30. Alexandru G. Bardas and Xinming Ou. Setting up and using a cyber security lab for education purposes. *Journal of Computing Sciences in Colleges*, Vol. 28, Issue 5, May 2013.
31. Justin Yackoski, Jason Li, Scott A. DeLoach, and Xinming Ou. Mission-oriented moving target defense based on cryptographically strong network dynamics. *Proceedings of the 8th Annual Cyber Security and Information Intelligence Research Workshop (CSIIRW)*, Oak Ridge, TN, USA, January. 2013.
32. Dan Moor, S. Raj Rajagopalan, Sathya Chandran Sundaramurthy, and Xinming Ou. Investigative response modeling and predictive data collection. *The seventh IEEE eCrime Researchers Summit (eCrime'12)*, Las Croabas, Puerto Rico, USA, October, 2012.
33. Rui Zhuang, Su Zhang, Scott A. DeLoach, Xinming Ou, and Anoop Singhal. Simulation-based approaches to studying effectiveness of moving-target network defense. *National Symposium on Moving Target Research*, Annapolis, MD, USA, June, 2012.
34. Alexandru G. Bardas, Loai Zomlot, Sathya Chandran Sundaramurthy, Xinming Ou, S. Raj Rajagopalan, and Marc R. Eisenbarth. Classification of UDP traffic for DDoS detection. *5th USENIX*

Workshop on Large-Scale Exploits and Emergent Threats (LEET), San Jose, CA, USA, April, 2012.

35. Torben Amtoft, Josiah Dodds, Zhi Zhang, Andrew Appel, Lennart Beringer, John Hatcliff, Xinming Ou, and Andrew Cousino. A certificate infrastructure for machine-checked proofs of conditional information flow. *First conference on Principles of Security and Trust (POST'12, part of ETAPS 2012)*, Tallinn, Estonia, March 2012. (Acceptance rate: 30%)
36. Heqing Huang, Su Zhang, Xinming Ou, Atul Prakash, and Karem Sakallah. Distilling critical attack graph surface iteratively through minimum-cost SAT solving. *27th Annual Computer Security Applications Conference (ACSAC)*, Orlando, FL, USA, Dec. 2011. (**Best Student Paper Award**. Acceptance rate: 20%)
37. Loai Zomlot, Sathya Chandran Sundaramurthy, Kui Luo, Xinming Ou, and S. Raj Rajagopalan. Prioritizing intrusion analysis using Dempster-Shafer theory. *4TH ACM Workshop on Artificial Intelligence and Security (AISec)*, Chicago, USA, Oct. 2011.
38. Xinming Ou and Anoop Singhal. Quantitative security risk assessment of enterprise networks. *SpringerBrief Series, Information Security.* Nov. 2011.
39. Anoop Singhal and Xinming Ou. Security risk analysis of enterprise networks using probabilistic attack graphs. NIST Interagency Report 7788. Aug. 2011.
40. Su Zhang, Doina Caragea, and Xinming Ou. An empirical study of using the National Vulnerability Database to predict software vulnerabilities. *22nd International Conference on Database and Expert Systems Applications (DEXA)*, Toulouse, France, August 2011. (Acceptance rate: 25%)
41. Sathya Chandran Sundaramurthy, Loai Zomlot, and Xinming Ou. Practical IDS alert correlation in the face of dynamic threats. *The 2011 International Conference on Security and Management (SAM)*, Las Vegas, USA, July 2011. (Acceptance rate: 23%)
42. Su Zhang, Xinming Ou, Anoop Singhal and John Homer. An empirical study of a vulnerability metric aggregation method. *The 2011 International Conference on Security and Management (SAM'11), special track on Mission Assurance and Critical Infrastructure Protection (STMACIP'11)*, Las Vegas, USA, July 2011. (Acceptance rate: 23%)
43. Su Zhang, Xinming Ou, and John Homer. Effective network vulnerability assessment through model abstraction. *The Eighth Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA)*, Amsterdam, The Netherlands, July 2011. (Acceptance rate: 32%)
44. Peng Xie, Jason H Li, Xinming Ou, Peng Liu, and Renato Levy. Using Bayesian networks for cyber security analysis. *The 40th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, Chicago, USA, June 2010. (Acceptance rate: 23%)
45. Xinming Ou, S. Raj Rajagopalan, and Sakthiyuvaraja Sakthivelmurugan. An empirical approach to modeling uncertainty in intrusion analysis. In *25th Annual Computer Security Applications Conference (ACSAC)*, Honolulu, Hawaii, USA, Dec 2009. (Acceptance rate: 20%)
46. Jason Li, Xinming Ou, and Raj Rajagopalan. Uncertainty and risk management in cyber situational awareness. In Sushil Jajodia, editor, *Cyber Situational Awareness*, chapter 3. Springer, Nov. 2009.
47. Abhishek Rakshit and Xinming Ou. A host-based security assessment architecture for industrial control systems. In *2nd International Symposium on Resilient Control Systems (ISRCS)*, Idaho Falls, ID, USA, August 2009.
48. John Homer and Xinming Ou. SAT-solving approaches to context-aware enterprise network security management. *IEEE JSAC Special Issue on Network Infrastructure Configuration*, 27(3), April, 2009. (Acceptance rate: 25%)
49. Anoop Singhal and Xinming Ou. Techniques for enterprise network security metrics. In *5th Annual Workshop on Cyber Security and Information Intelligence Research: Cyber Security and Information Intelligence Challenges and Strategies (CSIIRW)*, Extended Abstract, April, 2009.
50. Reginald Sawilla and Xinming Ou. Identifying critical attack assets in dependency attack graphs. In *13th European Symposium on Research in Computer Security (ESORICS)*, Malaga, Spain, October

2008. (Acceptance rate: 22%)

51. John Homer, Ashok Varikuti, Xinming Ou, and Miles McQueen. Improving attack graph visualization through data reduction and attack grouping. In *The 5th International Workshop on Visualization for Cyber Security (VizSEC)*, Cambridge, MA, USA, September 2008.
52. Xinming Ou, Wayne Boyer, and Miles McQueen. A scalable approach to attack graph generation. In *13th ACM Conference on Computer and Communications Security (CCS)*, Alexandria, VA, USA, October 2006. (Acceptance rate: 15%)
53. Xinming Ou, Anna Squicciarini, Sebastien Goasguen, and Elisa Bertino. Authorization strategies for virtualized environments in grid computing systems. In *IEEE Workshop on Web Services Security (WSSS)*, Berkeley, California, USA, May, 2006.
54. Xinming Ou, Sudhakar Govindavajhala, and Andrew W. Appel. MulVAL: A logic-based network security analyzer. In *Proceedings of 14th USENIX Security Symposium*, Baltimore, Maryland, USA, 2005. (Acceptance rate: 15%)
55. K. Rustan M. Leino, Madan Musuvathi, and Xinming Ou. A two-tier technique for supporting quantifiers in a lazily proof-explicating theorem prover. In *Proceedings of 11th International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS)*, Edinburgh, UK, 2005.
56. Xinming Ou, Gang Tan, Yitzhak Mandelbaum, and David Walker. Dynamic typing with dependent types. In *Proceedings of 3rd IFIP International Conference on Theoretical Computer Science (TCS)*, Toulouse, France, 2004.
57. Cormac Flanagan, Rajeev Joshi, Xinming Ou, and James B. Saxe. Theorem proving using lazy proof explication. In *Proceedings of 15th Computer-Aided Verification Conference (CAV)*, Boulder, CO, USA, 2003.
58. Gang Tan, Xinming Ou and David Walker. Enforcing resource usage protocols via scoped methods. In *Proceedings of 10th International Workshop on Foundations of Object-Oriented Languages (FOOL)*, New Orleans, LA, USA, 2003 .
59. Wei Liu, Min Wu, Xinming Ou, Weimin Zheng, and Meiming Shen. Design of an I/O Balancing File System on Web Server Clusters. In *Proceedings of the 2000 International Workshop on Parallel Processing*, Toronto, Canada, August 2000.
60. Wei Liu, Weimin Zheng, Meiming Shen, Xinming Ou, and Min Wu. An Effective File Migration Algorithm in Cluster File Systems. In *Proceedings of the 2000 International Workshop on Parallel Processing*, Toronto, Canada, August 2000.

Professional Services

- Keynote speaker. The Third International Workshop on Graphical Models for Security (GraMSec), 2016
- Invited participant. MC2 Workshop on Data-Driven Approaches to Security and Privacy, Jan 8-9, 2015.
- Invited expert. ARO Workshop: "Cyber Security: From Tactics to Strategies and Back," Sept 23, 2014.
- Invited speaker. 1st Experimental Security Panoramas Workshop (ESP), August, 2011.
- Invited expert. 2nd ARO Workshop on Cyber Situation Awareness, March 3-5, 2009.
- Invited expert. NSF Workshop on Assurable and Usable Security Configuration, Aug 11-12, 2008.
- Panelist. Information and Cyberspace Symposium, U.S. Army Computer Network Operations - Electronic Warfare Proponent, Fort Leavenworth, Sept 22-25, 2008.
- Invited speaker. USENIX LISA Configuration Workshop, Nov 12, 2007.
- Panelist. National Science Foundation. 2010, 2011, 2014.
- Reviewer. U.S. Army Research Office (ARO), 2014.

- Reviewer. U.S. Air Force Office of Scientific Research (AFOSR), 2009, 2010.
- Poster and Demo Co-Chair. ACM Conference on Computer and Communications Security (CCS), 2009, 2010, 2014, 2015.
- Steering Committee member. Central Area Networking and Security Workshop (CANSec), 2012-2016.
- Tutorial speaker. ACM Conference on Computer and Communications Security (ACM CCS) 2009, 2010.
- Tutorial speaker. Annual Computer Security Applications Conference (ACSAC) 2011, 2012.
- TPC Co-Chair, 5th Symposium on Configuration Analytics and Automation (SafeConfig 2012).
- TPC Co-Chair, ACM Workshop on Moving Target Defense (MTD), 2017.
- TPC Co-Chair, IEEE CNS Network Forensics Workshop, 2016, 2017.
- Technical Program Committee member.
  - Annual Computer Security Applications Conference (ACSAC), 2013, 2014, 2016, 2017.
  - ACM Conference on Computer and Communications Security (CCS), 2015, 2016.
  - ACM Symposium on Information, Computer and Communications Security (ASIACCS), 2014, 2015.
  - IEEE International Workshop on Cyber-Physical Systems Security (CPS-Sec), 2017.
  - The Fourth International Workshop on Graphical Models for Security (GraMSec), 2017.
  - ACM Workshop on Moving Target Defense (MTD) 2014, 2015, 2016.
  - ACM Workshop on Cyber-Physical Systems Security & Privacy (CPS-SPC), 2016, 2017.
  - ACM Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM), 2016.
  - International Conference on Network and System Security (NSS), 2010, 2015.
  - International Conference on Information Security and Cryptology (Inscrypt), 2013, 2014.
  - 9th International Conference on Risks and Security of Internet and Systems (CRiSIS), 2014.
  - Machine Learning Challenges in Cyber Security Applications, Special Session at ICMLA 2013.
  - Conference on Privacy, Security and Trust (PST) 2011, 2013, 2014.
  - International Symposium on Resilient Control Systems (ISRCS) 2010, 2011, 2012, 2013.
  - Symposium on Security Analytics and Automation (SafeConfig) 2009, 2010, 2011, 2013, 2014.
- Reviewer for journals and conferences.
  - ACM Transactions on Privacy and Security (TOPS)
  - IEEE Transactions on Dependable and Secure Computing (TDSC)
  - Transactions on Information Forensics & Security
  - Journal of Computer Security
  - IEEE Security & Privacy
  - Security and Communication Networks
  - Journal of Network and Systems Management (JNSM) - Special Issue on Security Configuration Management
  - IEEE Journal on Selected Areas in Communications (JSAC) - Special Issue on Network Infrastructure Configuration
  - International Journal of Security and Networks (IJSN)
  - International Journal of Information Security
  - IET Information Security
  - Future Internet
  - ACM Transactions on Intelligent Systems and Technology (TIST)
  - Statistical Analysis and Data Mining (SAM)
  - USENIX Security Symposium (2014)
  - John Wiley & Sons

- ACM Conference on Computer and Communications Security (CCS 2011)
- ACM SIGPLAN International Conference on Object-Oriented Programming, Systems, Languages, and Applications (OOPSLA) 2009
- Workshop on Assurable & Usable Security Configuration (SafeConfig) 2009
- International Symposium on Resilient Control Systems (ISRCS) 2009
- Military Communications Conference (MilComm) 2008
- Network & Distributed System Security Symposium (NDSS) 2007