Xinming (Simon) Ou

Curriculum Vitae

Computer Science and Engineering
University of South Florida, ENB 339
4202 East Fowler Avenue
Tampa, FL 33620-5399

Office: (813)-974-4522
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**,
  Director, USF Rapid7 Cyber Threat Intelligence Lab, May 2023 – present
  Associate Chair of Graduate Affairs, Jan 2021 – Aug 2022
  Professor, Aug 2018 – present
  Associate Professor, Aug 2015 – July 2018.
- **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. Mixed Methods Research on Expert Cyber Training Using a Mock SOC (PI). Office of Naval Research. $754,721, 6/1/2023-5/31/2026.
2. CyberCorps Scholarship for Service: Cybersecurity Research and Education for Service in Government (CREST) (co-PI). National Science Foundation. $4,460,826, 1/1/2023-12/31/2027.
3. SaTC: CORE: Medium: Collaborative: Understanding Security in the Software Development Lifecycle: A Holistic, Mixed-Methods Approach (PI). National Science Foundation. $500,000, 9/1/2018-8/31/2022.
4. 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 - 8/31/2022.

5. SaTC: CORE: Small: Collaborative: Data-driven Approaches for Large-scale Security Analysis of Mobile Applications (PI). National Science Foundation. $200,000, 8/15/2017-8/14/2021.
6. A Reinforcement Learning Approach to Detecting Persistent Threats (co-PI). Cyber Florida. $75,000, 7/1/2018-12/31/2019.
7. ALCHEMI: Attacker Learning in Cybernetworks using Heterogeneous Energy-guided Model. U.S. Navy (through Aptima, Inc.). $42,000, 7/1/2019- 12/9/2019.
8. 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*.)
9. 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.
10. 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.
11. MRI: Acquisition of an Adaptive Data Cluster for Data-intensive Applications in Science and Engineering (co-PI). National Science Foundation. $300,000, 9/1/2014-8/31/2017.
12. TWC SBE TTP: Medium: Bringing Anthropology into Cybersecurity (PI). National Science Foundation. $715,845, 9/1/2013-8/31/2017.
13. 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.
14. CAREER: Reasoning under Uncertainty in Cybersecurity (PI). National Science Foundation. $457,373, 3/1/2010 - 2/28/2017.
15. 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.
16. 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.
17. 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.
18. 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.
19. TC:Small:Collaborative Research:Models and Techniques for Enterprise Network Security Metrics (PI). National Science Foundation. $396,676, 10/1/2010-9/30/2014.
20. Cyber-security partnership between Kansas State University and CABEM/NTS (co-PI). National Technical Systems. $98,000, 02/01/2011-01/31/2012.
21. A New Approach to Rigorous Risk Analytics using Attack Graphs (PI). HP Labs Innovation Research Program. $220,716, 8/1/2010-7/31/2013.
22. CT-ISG: Model-Based, Automatic Network Security Management (PI). National Science Foundation. $245,000+$13,500 REU, 8/1/2007 - 7/31/2010.
23. 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.
24. A Domain Specific Language for Defining High-Assurance Secure Network Guards (co-PI). Rockwell Collins, Inc. $170,000, 9/22/2008 - 8/31/2009.
25. 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. Kumar Shashwat, Francis Hahn, Xinming Ou, Dmitry Goldgof, Jay Ligatti, Lawrence Hall, S. Raj Rajagopalan, and Armin Ziaie Tabari. A preliminary study on using large language models in software pentesting. In *Workshop on SOC Operations and Construction (WOSOC)*, March, 2024.
2. Kumar Shashwat, Francis Hahn, Xinming Ou, and Anoop Singhal. Security analysis of trust on the controller in the Matter protocol specification. In *IEEE Conference on Communications and Network Security, Cyber-physical Systems Security Workshop*, Oct, 2023.
3. Armin Ziaie Tabari, Guojun Liu, Xinming Ou, and Anoop Singhal. Revealing human attacker behaviors using an adaptive Internet of Things honeypot ecosystem. In *Peterson, G., Shenoi, S. (eds) Advances in Digital Forensics XIX. DigitalForensics 2023. IFIP Advances in Information and Communication Technology, vol 687. Springer, Cham.*, Oct, 2023.
4. Daniel Lende, Alexis Monkhouse, Jay Ligatti, and Xinming Ou. Co-creation in secure software development: Applied ethnography and the interface of software and development. *Human Organization*, 82(1), March, 2023.
5. Soumyadeep Hore, Fariha Moomtaheen, Ankit Shah, and Xinming Ou. Towards optimal triage and mitigation of context-sensitive cyber vulnerabilities. *IEEE Transactions on Dependable and Secure Computing (TDSC)*, Feb 2022.
6. Anwesh Tuladhar, Daniel Lende, Jay Ligatti, and Xinming Ou. An analysis of the role of situated learning in starting a security culture in a software company. In *Seventeenth Symposium on Usable Privacy and Security (SOUPS)*, Aug 2021. (**Distinguished Paper Award**. Acceptance rate: 26.5%)
7. Shima Mohebbi, Qiong Zhang, E Christian Wells, Tingting Zhao, Hung Nguyen, Mingyang Li, Noha Abdel-Mottaleb, Shihab Uddin, Qing Lu, Mathews J Wakhungu, Zhiqiang Wu, Yu Zhang, Anwesh Tuladhar, and Xinming Ou. Cyber-physical-social interdependencies and organizational resilience: A review of water, transportation, and cyber infrastructure systems and processes. *Sustainable Cities and Society*, Vol 62, Nov 2020.
8. Hernan Palombo, Armin Ziaie Tabari, Daniel Lende, Jay Ligatti, and Xinming Ou. An ethnographic understanding of software (in)security and a co-creation model to improve secure software development. In *Sixteenth Symposium on Usable Privacy and Security (SOUPS)*, Aug, 2020. (Acceptance rate: 19.8%)
9. Dewan Chaulagain, Prabesh Poudel, Prabesh Pathak, Sankardas Roy, Doina Caragea, Guojun Liu, and Xinming Ou. Hybrid analysis of Android apps for security vetting using deep learning. In *IEEE Conference on Communications and Network Security (CNS)*, June, 2020.
10. Xiaodong Yu, Fengguo Wei, Xinming Ou, Michela Becchi, Tekin Bicer, and Danfeng Yao. GPU-based static data-flow analysis for fast and scalable Android app vetting. In *IEEE International Symposium on Parallel and Distributed Processing (IPDPS)*, May, 2020.
11. Yuping Li, Doina Caragea, Lawrence Hall, and Xinming Ou. Experimental study of machine learning based malware detection systems' practical utility. In *HICSS Symposium on Cybersecurity Big Data Analytics*, Wailea, Hawaii, U.S.A, Jan 2020.
12. Yuping Li, Jiyong Jang, and Xinming Ou. Topology-aware hashing for effective control flow graph similarity analysis. In *15th EAI International Conference on Security and Privacy in Communication Networks (SecureComm)*, Orlando, U.S.A., Oct 2019.
13. Fengguo Wei, Xingwei Lin, Xinming Ou, Ting Chen, and Xiaosong Zhang. JNSAF: Precise and efficient NDK/JNI-aware inter-language static analysis framework for security vetting of Android applications with native code. In *25th ACM Conference on Computer and Communications Security (CCS)*, Toronto, Canada, Oct 2018. (Acceptance rate: 16.6%)
14. 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. *ACM Transactions on*

Privacy and Security (TOPS), 21(3), June 2018.

15. Yaohui Chen, Yuping Li, Long Lu, Yueh-Hsun Lin, Hayawardh Vijayakumar, Zhi Wang, and Xinming Ou. InstaGuard: Instantly deployable hot-patches for vulnerable system programs on Android. In *The Network and Distributed System Security Symposium (NDSS)*, San Diego, CA, Feb 18-21, 2018.
16. 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%)
17. 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%) Open-source tool release: http://arguslab.github.io/ancor/
18. 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%)
19. 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 International Workshop on Communication, Computing, and Networking in Cyber Physical Systems (CCNCPS 2017)*, Atlanta, GA, USA, June 5, 2017.
20. 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.
21. 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.
22. 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.
23. 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.
24. 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.13, July-Aug 2016.
25. 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%)
26. 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%)
27. 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.
28. 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%)
29. 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.

30. 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.
31. 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.
32. 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%)
33. 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%)
34. 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%)
35. 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%)
36. 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%) Open-source tool release: http://pag.arguslab.org/argus-saf
37. 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.
38. 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.
39. 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%)
40. 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.
41. 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.
42. 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%)
43. 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.

44. 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.
45. 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.
46. 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.
47. 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.
48. 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.
49. 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.
50. 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%)
51. 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%)
52. 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.
53. Xinming Ou and Anoop Singhal. Quantitative security risk assessment of enterprise networks. *SpringerBrief Series, Information Security.* Nov. 2011.
54. Anoop Singhal and Xinming Ou. Security risk analysis of enterprise networks using probabilistic attack graphs. NIST Interagency Report 7788. Aug. 2011.
55. 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%)
56. 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%)
57. 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%)
58. 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%)
59. 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%) **Awarded DSN Test of Time Award, 2020.**

60. 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%) Open-source tool release: http://www.arguslab.org/snips.html
61. 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.
62. 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.
63. 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%)
64. 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.
65. 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%)
66. 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.
67. 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%) Open-source tool release: http://www.arguslab.org/mulval.html
68. 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.
69. 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%)
70. 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.
71. 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.
72. 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.
73. 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 .
74. 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.

75. 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

- General Co-Chair. ACM Conference on Computer and Communications Security (CCS), 2020.
- Panel Co-Chair. EAI International Conference on Security and Privacy in Communication Networks (SecureComm), 2019.
- TPC Co-Chair, ACM Workshop on Moving Target Defense (MTD), 2017.
- TPC Co-Chair, IEEE CNS Network Forensics Workshop, 2016, 2017.
- Poster and Demo Co-Chair. ACM Conference on Computer and Communications Security (CCS), 2009, 2010, 2014, 2015.
- TPC Co-Chair, 5th Symposium on Configuration Analytics and Automation (SafeConfig 2012).
- Technical Program Committee member.
  - NDSS Workshop on SOC Operations and Construction (WOSOC), 2023, 2024.
  - IEEE Conference on Communications and Network Security (CNS), 2022.
  - 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, 2022.
  - 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.
- Steering Committee member. ACM Workshop on Moving Target Defense (MTD), 2014 - present.
- Steering Committee member. Central Area Networking and Security Workshop (CANSec), 2012-2016.
- Keynote speaker. The Third International Workshop on Graphical Models for Security (GraMSec), 2016
- Panelist. National Science Foundation.
- Reviewer. U.S. Army Research Office (ARO).
- Reviewer. U.S. Air Force Office of Scientific Research (AFOSR).
- 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
- Journal of Network and Computer Applications
- 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
- John Wiley & Sons
- ACM Conference on Computer and Communications Security
- ACM SIGPLAN International Conference on Object-Oriented Programming, Systems, Languages, and Applications (OOPSLA)
- Workshop on Assurable & Usable Security Configuration (SafeConfig)
- International Symposium on Resilient Control Systems (ISRCS)
- Military Communications Conference (MilComm)
- Network & Distributed System Security Symposium (NDSS)