Meng Yu, Ph.D.

Associate Dean and Professor, School of Natural and Social Sciences, Lehman College, CUNY

ABET PEV | NSA/DHS CAE Mentor/Reviewer

Web: http://www.profmengyu.org

Executive Profile

Academic administrator, tenured professor, and cybersecurity/AI scholar with leadership experience across associate dean, department chair, program director, center director, and faculty governance roles. Experienced in building academic programs and departments, leading accreditation and CAE designation work, growing enrollment capacity, hiring faculty, supporting sponsored programs, and developing external partnerships across public, private, R1, R2, RCU, and minority-serving institutions.

Professional Highlights

- Senior academic leader with experience as Associate Dean, Department Chair, Associate Chair, Program Director, Center Director, and tenured Full Professor, including service as the Robert Miner Endowed Chair at Roosevelt University.
- Department builder and inaugural chair who merged academic units, launched a new cybersecurity department, hired tenure/tenure-track faculty, and expanded the department to approximately 15 faculty and 700 students in two years.
- Led academic programs across Computer Science, Information Technology, Data Science, Cybersecurity, and interdisciplinary Music and Computing, including B.S., B.A., M.S., and Ph.D. programs.
- Developed graduate, undergraduate, accelerated, interdisciplinary, cross-unit, and joint programs, including two on-campus M.S. cybersecurity programs, a B.A. in Music and Computing, and twelve BS-to-MS accelerated pathways.
- Led and supported accreditation, assessment, and designation efforts involving ABET, NSA/DHS CAE-CD, CAE-Cyber AI, SACSCOC, and HLC; ABET Program Evaluator and CAE Mentor/Reviewer.
- Led efforts for NSA/DHS CAE Cyber AI pilot designation, one of twelve nationwide, managed CAE-CD program work, and contributed to CAE-CO designation efforts at UTSA.
- Built industry partnerships, industrial advisory boards, and external collaborations with major research universities, federal sponsors, and technology organizations.
- Secured and supported competitive grants and sponsored programs from NSF SaTC, ARO, NSF EDU, DoD CySP, and other federal agencies.
- Contributed to university-level enrollment, marketing, retention, curriculum, graduate education, undergraduate education, research, and institutional transition initiatives.
- Leadership experience across public, private, large, small, R1/R2/RCU, and minority-serving higher education institutions.

Education

Postdoctoral Training	Cyber Security Lab	07/02-08/04
	The Pennsylvania State University, University Park, USA	
	Advisor: Professor Peng Liu	
	University of Maryland, Baltimore County, USA	01/02-06/02
	Advisor: Professor Peng Liu	
Doctor of Philosophy	Department of Computer Science	December, 2001
	Nanjing University, China	
	Advisor: Professor Li Xie, and Professor Zhongxiu Sun, Member of Chinese Academy of Science.	
Master of Science	Department of Computer Science	March, 1998
	Northeastern University, China	
	Advisor: Professor Tianshun Yao.	

Training and Professional Development

2025 ABET Advanced Program Assessment workshop.
2025 NSA/DHS CAE Cyber AI Program Evaluator and Mentor training.
2025 ABET Program Evaluator (PEV) training.
2024 NSA/DHS CAE Competency Requirements training.
2024 NVIDIA faculty AI training certificate: Fundamentals of Deep Learning.
2024 NVIDIA faculty AI training certificate: Generative AI with Diffusion Models
2024 NVIDIA faculty AI training certificate: Building Transformer-Based Natural Language Processing Applications.
2024 ABET Fundamentals of Program Assessment workshop.
2013 NSF I-Corps Technology Commercialization Training.

Employment and Experience

08/2026-present Professor with Tenure and Associate Dean
School of Natural and Social Sciences
Department of Computer Science
Lehman College, CUNY (Carnegie RCU)

08/2025-06/2026 Associate Professor (with tenure)
Computer Science
Governors State University (Carnegie R2)
Key achievements: Advanced research initiatives in AI for cybersecurity and AI for music.

01/2024-07/2025	Professor (with tenure) Department Chair (Inaugural Chair) Department of Cybersecurity and Information Technology (merged from two departments) University of West Florida (Carnegie R2) *Key achievements:* Built a new cybersecurity department by merging IT-related units; led strategic expansion to approximately 700 students and 15 faculty; hired five tenure/tenure-track faculty in two years; led NSA/DHS CAE-Cyber AI Pilot Program designation efforts (1 of 12 nationwide); launched an on-campus M.S. in Cybersecurity; managed an NSA/DHS CAE-CD program; led ABET, CAE-CD, and SACSCOC reviews; built an industrial advisory board (IAB); and supported two clean-pass ABET site visits with no shortcomings for two undergraduate programs.
08/2023-11/2023	Professor (with tenure) Department Chair (Inaugural Chair) Department of Cybersecurity University of West Florida (Carnegie R2)
08/2018-07/2023	Professor (with tenure), Robert Miner Endowed Chair Department Chair *Appointed through national search as Department Chair in 2018 and reappointed for a second term in 2021.* Department of Computer Science, Information Technology, and Data Science Roosevelt University *Key achievements:* Launched new M.S. in Cybersecurity and B.A. in Music & Computing programs; led NSA/DHS CAE-CD and CAE-C redesignation and HLC program review; secured DoD CySP grants; and built an industrial advisory board.
08/2020-07/2023	Center Director NSA/DHS National Center of Academic Excellence in Cyber Defense (CAE-CD) Roosevelt University
08/2019-07/2023	Program Co-Director B.A. in Music & Computing Program Collaboration with Chicago College of Performing Arts (CCPA) Roosevelt University
08/2015-07/2018	Associate Professor (with tenure) Chair of Master's Program Committee Department of Computer Science University of Texas at San Antonio (Carnegie R2 at the time of employment, now R1) *Key achievements:* Supported NSA/DHS CAE-CO designation (the 7th nationwide) and ABET work; secured NSF and ARO grants; built CAE-CO-aligned core curriculum; and managed graduate program enrollment.

08/2010-06/2015	Co-Director of the graduate program M.S. in Computer and Information System Security Program A joint M.S. program with School of Business Virginia Commonwealth University (Carnegie R1) *Key achievements:* Supported ABET accreditation; managed a joint M.S. in Cybersecurity and Ph.D./M.S. in Computer Science programs; and secured NSF grants.
08/2013-07/2014	Graduate Program Director Department of Computer Science Virginia Commonwealth University (Carnegie R1)
08/2012-07/2013	Associate Chair of the Computer Science Department Department of Computer Science Virginia Commonwealth University (Carnegie R1)
08/2010-06/2015	Associate Professor (tenure granted in 2012) Department of Computer Science Virginia Commonwealth University (Carnegie R1)
08/2007-06/2010	Assistant Professor Department of Computer Science Western Illinois University *Key achievements:* Secured NSF grants and developed new cybersecurity curriculum.
08/2006-06/2007	Co-Director of the graduate program Department of Computer Science Monmouth University *Key achievements:* Created a new cybersecurity concentration, managed M.S. in Computer Science enrollment, and secured an NSF grant.
08/2004-06/2007	Assistant Professor Department of Computer Science Monmouth University
07/2002-08/2004	Postdoctoral Research Associate School of Information Sciences and Technology Pennsylvania State University, University Park
12/2001-06/2002	Postdoctoral Research Associate Department of Information System University of Maryland, Baltimore County
04/1998-12/2001	Faculty Member Department of Computer Science Nanjing University, China Faculty Member National Key Laboratory for Novel Software Technology, China.
08/2000-12/2001	Technical Consultant Jiangsu Nandasoft Co, Ltd. Nanjing, China

08/1992-08/1995 Project Manager
CAPO Computer Techniques Company, Liaoning, China.

RESEARCH

4.1 Research Interests

Computer Security: — *secure computing architecture, system security*,
— *cloud computing, virtualization platform and security*,
— *intrusion tolerance, self-healing systems, data integrity*.
Artificial Intelligence: — *music AI*, *AI in music*.
— *trustworthy AI*, *AI for security*.

4.2 Funded Research Grants

- Lead Principal Investigator. *TWC: Small: Collaborative: Towards Agile and Privacy-Preserving Cloud Computing*. SaTC, NSF. $500K ($250K for UTSA). October 2015 - September 2018. Award number: 1634441.
- Moving Target Defense Through Dynamic Virtual Machine Placement in Clouds. ARO. $15K, 2014-2017. Subcontracted from TAMUSA.
- Principal Investigator. *I-Corps: Commercializing a privacy-preserving cloud computing platform*. I-Corps, NSF. $50K. July 2013 - December 2014. Award number: 1342664.
- Principal Investigator. *TC:EAGER:New Privacy Preserving Architecture for Security Monitoring in Cloud Computing*. Trustworthy Computing, NSF. $200K. January 2011 - December 2014. Award number: 1100221.
- Principal Investigator at WIU (with Dr. Sushil Jajodia, Lead PI at GMU, and Dr. Peng Liu, PI at PSU), *TC: Medium: Collaborative Research: Towards Self-Protecting Data Centers: A Systematic Approach*, Trusted Computing, NSF. $1.2M. ($270K for Meng Yu), Sep. 2009 - Aug. 2012. Award number: 0905153.
- Principal Investigator at WIU (with Dr. Wanyu Zang, Co-PI at WIU, Dr. Peng Liu, Lead PI at PSU, and Dr. Qijun Gu, PI at Texas State University). *NeTS:Small:Collaborative Research:Secure and Resilient Channel Allocation in Multi-Radio Wireless Networks*, Trusted Computing, NSF. $300K ($90K for Meng Yu). Sep. 2009 - Aug. 2012. Award number: 0916000.
- Principal Investigator at WIU (with Professor Peng Liu, Lead PI, at The Pennsylvania State University, and Professor Sushil Jajodia, PI, at George Mason University), *CT-ISG: New theories and techniques for non-blocking on-line recovery from database corruption attacks*, CyberTrust, NSF. $150K. ($34K. for Meng Yu). Sep. 2007- Aug, 2009. Award number: 0757210.
- Principal Investigator, *Create trustiness based on multi-level authentication and integrity in distributed systems*, through the Center for Rapid Response Database Systems (CRRDS) by School of Science, Technology, and Engineering, Monmouth University, Summer research support, $15,000, 2006

4.3 Education Grants

- Co-PI, *DoD Cyber Scholarship Program (CySP)*. $87,979. August, 2023 - July, 2024.
- Co-PI, *DoD Cyber Scholarship Program (CySP)*. $95,072. August, 2022 - July, 2023.

- Principal Investigator. *EDU: Collaborative: Integrating Embedded Systems Security into Computer Engineering and Science Curricula*. SaTC NSF. $50K. September, 2016 - August, 2019. Award number: 1623247.

4.4 Publications

The complete publication record is retained below. The body of work spans system security, trusted computing, cloud and virtualization security, intrusion tolerance, database recovery, wireless/network security, and AI-enabled cyber defense, with peer-reviewed conference, journal, book-chapter, and invited outputs.

4.4.1 Refereed Conference and Workshop Publications

1. Prasad Calyam, Mayank Kejriwal, Kannappan Palaniappan, Vijay Anand, Bharat Bhargava, Jianlin Cheng, Weichao Wang, Sanjay Kumar Madria, Kerk Kee, Rohit Chadha, Mukesh Singhal, Venkata Sriram Siddhardh Nadendla, Suranjan Panigrahi, Patrice Buzzanell, Meng Yu, Linquan Bai, and Sajal K. Das. "Towards a Domain-Agnostic Knowledge Graph-as-a-Service Infrastructure for Active Cyber Defense with Intelligent Agents." In *Proceedings of The 52nd IEEE Applied Imagery Pattern Recognition Workshop*. Saint Louis, MO Sept 27-29, 2023
2. Naiwei Liu, Meng Yu, Wanyu Zang and Ravi Sandhu, "On the Cost-Effectiveness of TrustZone Defense on ARM Platform." In *Proceedings of 21st World Conference on Information Security Applications (WISA)*, Virtual Event, August 26-28, 2020,
3. Li Liu, An Wang, Wanyu Zang, Meng Yu, Mengbai Xiao and Songqing Chen. "Shuffler: Mitigate Cross-VM Side-channel Attacks via Hypervisor Scheduling." In *The 2018 International Conference on Security and Privacy in Communication Networks (SECURECOMM)*. August 8-10, 2018. Singapore, Singapore.
4. Li Liu, An Wang, Wanyu Zang, Meng Yu, Songqing Chen. "Empirical Evaluation of the Hypervisor Scheduling on Side Channel Attacks." In *IEEE ICC 2018 Communication and Information Systems Security Symposium*. 20-24 May 2018. Kansas City, MO, USA.
5. Le Guan, Peng Liu, Xinyu Xing, Xinyang Ge, Shengzhi Zhang, Meng Yu, Trent Jaeger. "TrustShadow: Secure Execution of Unmodified Applications with ARM TrustZone." In *The 15th ACM International Conference on Mobile Systems (MobiSys 2017)*. June 19th - 23rd, 2017. Niagara Falls, NY, USA.
6. Jin Han, Wanyu Zang, Songqing Chen, Meng Yu. "Reducing Security Risks of Clouds through Virtual Machine Placement." In *The 31st Annual WG 11.3 Conference on Data and Applications Security and Privacy (DBSec'17)*. July 19th - 21st. Philadelphia, PA, USA.
7. Zili Zha, Min Li, Wanyu Zang, Meng Yu, Songqing Chen. "AppGuard: A Hardware Virtualization Based Approach on Protecting User Applications from Untrusted Commodity Operating System." In *2015 International Conference on Computing, Networking and Communications (Invited Position Paper)*. February 16-19, 2015. Anaheim, California, USA.
8. Min Li, Zili Zha, Wanyu Zang, Meng Yu, Peng Liu, Kun Bai. "Detangling Resource Management Functions from the TCB in Privacy-Preserving Virtualization." In *The 19th European Symposium on Research in Computer Security (ESORICS 2014)*. September 7-11, 2014, Wroclaw, Poland. Acceptance rate: 20%.
9. Bin Wang, Xiaochun Yang, Wanyu Zang and Meng Yu. "Approximate Self-Adaptive Data Collection in Wireless Sensor Networks." In *The 9th International Conference on Wireless Algorithms, Systems, and Applications (WASA 2014)*. June 23-25, 2014, Harbin, China.
10. Min Li, Wanyu Zang, Kun Bai, Meng Yu, Peng Liu. "MyCloud – Supporting User-Configured Privacy Protection in Cloud Computing." In *Annual Computer Security Applications Conference*. New Orleans, Louisiana USA, December 2013. Acceptance rate: 19%.

11. Qijun Gu, Kyle Jones, Wanyu Zang, Meng Yu and Peng Liu. "Revealing Abuses of Channel Assignment Protocols in Multi-Channel Wireless Networks: An Investigation Logic Approach." In *The 17th European Symposium on Research in Computer Security (ESORICS 2012)*. Acceptance rate: 20%.
12. Xiangyu Liu, Bin Wang, Xiaochun Yang, Meng Yu and Wanyu Zang. "Obtaining K-Obfuscation for Profile Privacy in Social Networks." In *The 7th International Conference on Frontier of Computer Science and Technology (FCST)* TSP Track, Suzhou, China, November 21-23, 2012.
13. Min Li, Yulong Zhang, Kun Bai, Wanyu Zang, Meng Yu, Xubin He. "Improving Cloud Survivability through Dependency based Virtual Machine Placement (short paper)." In *The International Conference on Security and Cryptography (SECRYPT'12)*, Rome,Italy, 24-27 July 2012.
14. Qijun Gu, Wanyu Zang, Meng Yu, and Peng Liu. "Collaborative Traffic-aware Intrusion Monitoring in Multi-channel Mesh Networks." In *the 11th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom-2012)*, Liverpool, UK, 25-27 June 2012.
15. Wuqiong Pan, Yulong Zhang, Meng Yu, and Jiwu Jing. "Improving Virtualization Security by Splitting Hypervisor into Smaller Components." In *The 26th Annual WG 11.3 Conference on Data and Applications Security and Privacy (DBSec'12)*, Institut Mines-Télécom, Paris, France. July 11-13, 2012.
16. Yulong Zhang, Min Li, Kun Bai, Meng Yu, Wanyu Zang. "Incentive Compatible Moving Target Defense against VM-Colocation Attacks in Clouds." In *IFIP International Information Security and Privacy Conference 2012*, Heraklion, Crete, Greece, 4-6 June 2012. Acceptance rate: 25%.
17. Wuqiong Pan, Jiwu Jing, Luning Xia, Zongbin Liu, Meng Yu. "An efficient RSA Implementation without Precomputation". In *The 7th China International Conference on Information Security and Cryptology (Inscrypt'2011)*, Beijing, China, November 30 - Dec 3 2011.
18. Qijun Gu, Meng Yu, Wanyu Zang, and Peng Liu. "Lightweight attacks against channel assignment protocols in mimc wireless networks." In *IEEE ICC, Communication and Information System Security Symposium*, Kyoto, Japan, 5-9 June 2011. Acceptance rate: 38.5%.
19. Heywoong Kim, Qijun Gu, Meng Yu, Wangyu Zang, and Peng Liu."A simulation framework for performance analysis of multi-interface and multi-channel wireless networks in inet/omnet++." In *Proceedings of the 2010 Spring Simulation Multiconference, SpringSim'10*, pages 101:1-101:8, New York, NY, USA, 2010. ACM.
20. Meng Yu, Alex Hai Wang, Wanyu Zang, and Peng Liu. "Evaluating survivability and costs of three virtual machine based server architectures." In *International Conference on Security and Cryptography*, pages 478-485, 2010.
21. Wanyu Zang, Qijun Gu, Meng Yu, and Peng Liu. "An attack-resilient channel assignment mac protocol." In *Proceedings of the 2009 International Conference on Network-Based Information Systems, NBIS'09*, pages 246-253, Indianapolis, Indiana. USA, 2009. IEEE Computer Society. Acceptance rate: 37%.
22. Kun Bai, Meng Yu, and Peng Liu. "Trace: Zero-down-time database damage tracking, quarantine, and cleansing with negligible run-time overhead." In *Proceedings of the 13th European Symposium on Research in Computer Security: Computer Security, ESORICS'08*, pages 161-176, Berlin, Heidelberg, 2008. Springer-Verlag. Acceptance rate: 22%.
23. Meng Yu, Wanyu Zang, and Peng Liu. "Database isolation and filtering against data corruption attacks." In *Annual Computer Security Applications Conference*, pages 97-106, Miami, Florida, December 2007. Acceptance rate: 22%.
24. Meng Yu, Wanyu Zang, and Barbara Reagor. "Decentralized trust management based on the reputation of information sources." In *IEEE International Conference on Networking, Sensing and Control (ICNSC'2007)*, pages 212-217, 2007.

25. Wanyu Zang and Meng Yu. "A dead-lock free self-healing algorithm for distributed transactional processes." In *International Conference on Information systems security (ICISS'06)*, pages 289-302, December 2006. Acceptance rate: 30%.
26. Meng Yu, Wanyu Zang, and Peng Liu. "Defensive execution of transactional processes against attacks." In *Annual Computer Security Applications Conference (ACSAC'05)*, pages 515-526, Tucson, Arizona, USA, December 2005. Acceptance rate: 19.6%.
27. Meng Yu, Wanyu Zang, Peng Liu, and Jiacun Wang. "The architecture of an automatic distributed recovery system." In *IEEE International Conference on Networking, Sensing and Control*, pages 999-1004, Tucson, Arizona, 2005.
28. Meng Yu, Peng Liu, and Wanyu Zang. "Self-healing workflow systems under attacks." In *The 24th International Conference on Distributed Computing Systems (ICDCS'04)*, pages 418-425, 2004. Acceptance rate: 17.68%.
29. Meng Yu, Peng Liu, and Wanyu Zang. "Intrusion masking for distributed atomic operations." In *The 18th IFIP International Information Security Conference*, pages 229-240, Athens Chamber of Commerce and Industry, Greece, 26-28 May 2003. IFIP Technical Committee 11, Kluwer Academic Publishers. Acceptance rate: 27%.
30. Meng Yu, Peng Liu, and Wanyu Zang. "Multi-version based attack recovery of workflow." In *The 19th Annual Computer Security Applications Conference (ACSAC'03)*, pages 142-151, Las Vegas, Nevada, December 2003. Acceptance rate: 30%.
31. "JAPS-II: A Source to Source Parallelizing Compiler for Java". At the 2002 International Conference on Parallel and Distributed Processing Techniques and Applications (PDPTA'02), Las Vegas, June, 2002.

4.4.2 Refereed Journal Publications

32. Ganapathy Mani, Marina Haliem, Bharat Bhargava, Indu Manickam, Kevin Kochpatcharin, Myeongsu Kim, Eric Vugrin, Weichao Wang, Chris Jenkins, Pelin Angin and Meng Yu "Machine Learning Based Resilience Testing of an Address Randomization Cyber Defense." *IEEE Transactions on Dependable and Secure Computing*, 2023.
33. Jin Han, Wanyu Zang, Meng Yu and Ravi Sandhu, "Quantify Co-Residency Risks in the Cloud through Deep Learning." *IEEE Transactions on Dependable and Secure Computing*, Volume 18, Number 4, July 2021
34. Naiwei Liu, Meng Yu, Wanyu Zang, and Ravi Sandhu, "Cost and Effectiveness of TrustZone Defense and Side-Channel Attack on ARM Platform." *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, Volume 11, Number 4, Dec. 2020, pages 1-15
35. Naiwei Liu, Wanyu Zang, Songqing Chen, Meng Yu, Ravi Sandhu. "Adaptive Noise Injection against Side-Channel Attacks on ARM Platform." *EAI Endorsed Transactions on Security and Safety*, Vol 6, No. 19, 2019.
36. Le Guan, Peng Liu, Xinyu Xing, Xinyang Ge, Shengzhi Zhang, Meng Yu, Trent Jaeger. "Building a Trustworthy Execution Environment to Defeat Exploits from both Cyber Space and Physical Space for ARM." *IEEE Transactions on Dependable and Secure Computing*, Vol. 16, Issue 3, pages 438-453. 2018.
37. Jin Han, Wanyu Zang, Li Liu, Songqing Chen, Meng Yu. "Risk-aware Multi-Objectives Optimized Virtual Machine Placement in Cloud." *Journal of Computer Security*, Vol. 26, Issue 5, pages 707-730. 2018.
38. Bin Wang, Xiaochun Yang, Guoren Wang, Ge Yu, Wanyu Zang, Meng Yu. "Energy Efficient Approximate Self-Adaptive Data Collection in Wireless Sensor Networks." *Frontiers of Computer Science*, Vol-

ume 10, issue 5, page 936-950, October 2016.

39. David S Jackson, Wanyu Zang, Qijun Gu, Meng Yu. "Robust Detection of Rogue Signals in Cooperative Spectrum Sensing." *Journal of Internet Service and Information Security (JISIS)*, Vol. 5, No. 2, 2015.
40. David S Jackson, Wanyu Zang, Qijun Gu, Wei Cheng and Meng Yu. "Exploiting and Defending Trust Models in Cooperative Spectrum Sensing." *EURASIP Journal on Wireless Communications and Networking (Section: SI: Dynamic Spectrum Access for Throughput, Delay & Fairness Enhancement In Cognitive Radio Networks)*, 2015.
41. Xiangyu Liu, Bin Wang, Xiaochun Yang, Meng Yu and Wanyu Zang. "Obtaining K-Obfuscation for Profile Privacy in Social Networks." *Special issue of Security and Communication Networks (Wiley)*, 2014.
42. Shanchen Pang, Tan Li, Feng Dai, Meng Yu. "Particle Swarm Optimization Algorithm for Multi- salesman Problem with Time and Capacity Constraints." *Applied Mathematics & Information Sciences*. Vol. 7, No. 6, 2439-2444 2013. `http://dx.doi.org/10.12785/amis/070637`
43. Chengpo Mu, Meng Yu, Yingjiu Li, Wanyu Zang. "Risk balance defense approach against intrusions for network server." *International Journal of Information Security*. October 2013. `http://link.springer.com/article/10.1007%2Fs10207-013-0214-9.`
44. Yan Yang,Yulong Zhang,Alex Hai Wang, Meng Yu, Wanyu Zang,Peng Liu,Sushil Jajodia, "Quantitative survivability evaluation of three virtual machine-based server architectures." *Journal of Network and Computer Applications*. Volume 36, Issue 2, March 2013, Pages 781-790
45. Peng Liu and Meng Yu. "Damage assessment and repair in attack resilient distributed database systems." *Computer Standards and Interfaces*, 33:96-107, January 2011.
46. Meng Yu, Wanyu Zang, and Peng Liu. Recovery of data integrity under multi-tier architectures. IET Information Security, 4(4):344-351, 2010.
47. Meng Yu, Peng Liu, and Wanyu Zang. "The implementation and evaluation of a recovery system for workflows." *Journal of Network and Computer Applications*, 32:158-183, January 2009.
48. Wanyu Zang, Peng Liu, and Meng Yu. "How resilient is the internet against ddos attacks? — a game theoretic analysis of signature-based rate limiting." *The International Journal of Intelligent Control and Systems*, 12(4):307-316, December 2007.
49. Wanyu Zang, Meng Yu, and Peng Liu. "A distributed algorithm for workflow recovery." *International Journal on Intelligent Control and Systems*, 12(1):56-62, March 2007.
50. Peng Liu, Wanyu Zang, and Meng Yu. "Incentive-based modeling and inference of attacker intent, objectives, and strategies." *ACM Transaction on Information System Security*, 8:78-118, February 2005.
51. Meng Yu, Peng Liu, and Wanyu Zang. "Specifying and using intrusion masking models to process distributed operations." *Journal of Computer Security*, 13:623-658, July 2005.

4.4.3 Refereed Book Chapters

52. Wanyu Zang, Meng Yu, and Peng Liu. "Incentive-based methods for inferring attacker intent and strategies and measuring attack resilience." In H. Raghav Rao and Shambhu Upadhyaya, editors, *Handbooks in Information Systems: Information Assurance, Security and Privacy Services*, volume 4, pages 679-705. Emerald Group Publishing Limited, 2009.
53. Peng Liu, Sushil Jajodia, and Meng Yu. "Damage quarantine and recovery in data processing systems." In *Database Security Handbook: Applications and Trends*, pages 383-407. Springer, 2008.
54. Meng Yu, Peng Liu, Wanyu Zang, and Sushil Jajodia. "Trusted recovery." In Ting Yu and Sushil Jajodia, editors, *Secure data management in decentralized systems*, pages 59-94. Springer, 2007.

55. Peng Liu, Meng Yu, and Jiwu Jing. "Information assurance." In Hossein Bidgoli, editor, *Handbook of Information Security*, volume 2, pages 110-126. John Wiley & Sons, Inc., 2006.

4.4.4 Conference Proceedings (Co-Editor)

56. Qijun Gu, Wanyu Zang, and Meng Yu, "Security in Emerging Wireless Communication and Networking Systems (SEWCN)", Workshop 2009

4.4.5 Refereed Articles in Journals (*in Chinese*)

57. Meng Yu, Wanyu Zang, and Li Xie. "Parallelism Analysis based on Generalized Method Invocation Model". *The Chinese Journal of Computers, China*. pp. 403-408, April, 2002.
58. Meng Yu, Wanyu Zang, and Li Xie. "Method Invocation Localizing Optimization in Parallelizing Object-Oriented Language", *The Chinese Journal of Computers, China*. pp. 409-416, April, 2002.
59. Meng Yu, Ghuihai Chen, X. Yang, Li Xie, and Minyi Guo. "JAPS-II: A Parallelizing Compiler for Java". *Journal of Software, China*. 13 (4):739-747, 2002.
60. Meng Yu, Wanyu Zang, Li Xie, and Minyi Guo. "A Survey of Parallel Object-Oriented Language". *Journal of Software, China*. 12 (6):822-829 ,2001.
61. Xuelin Yang, Meng Yu, and Li Xie. "New Development of Automatic Parallel Compilation". *Journal of Software, China*, 11 (9):1268-1275 ,2000.
62. Xuelin Yang, Meng Yu, and Li Xie. "A Run-Time Technique for Parallel Loop Identification Based on Distributed System". *Journal of Software, China*. 13 (8):1718-1722 ,2002.
63. Wanyu Zang, Meng Yu, and Li Xie. "A Routing Protocol for Ad-hoc Mobile Network with Unidirectional Links (UAOR)". *The Chinese Journal of Computers, China*. No.10, pp. 1018-1025, 2001.
64. Wanyu Zang, Meng Yu, and Li Xie. "An Optimized Routing Protocol for Ad-hoc Mobile Network with Unidirectional Links (OUAOR)". *The Chinese Journal of Computers, China*. No. 10, pp. 1030-1037, 2002.
65. Wanyu Zang, Meng Yu, and Li Xie. "A Survey of On-demand Routing Protocols for Ad-hoc Mobile Networks". *The Chinese Journal of Computers, China*. pp. 1009-1017, 2002.
66. Wanyu Zang, Meng Yu, and Li Xie. "Stable Cluster Based Hybrid Routing Protocol for Ad-hoc Mobile Networks". *The Chinese Journal of Computers, China*. No.12, pp. 1262-1271, 2001.
67. Qing Gu, Daoxu Chen, and Meng Yu. "Validation Test of Distributed Program Based on Event Sequencing Constraints". *Journal of Software, China*. 11(8):1053-1059, 2000.
68. Meng Yu and Tianshun Yao, "A Hybrid Method for Collating Chinese Text: HMCTC", *Journal of Chinese Information, China*. No.1, 1998,

4.4.6 Technical Reports not Otherwise Published

1. Yulong Zhang, Wuqiong Pan, Qingpei Wang, Kun Bai, Meng Yu. Technical Report: "HypeBIOS: Enforcing VM Isolation with Minimized and Decomposed Cloud TCB." VCU CyberSecurity Lab. 2012.
2. Yulong Zhang, Min Li, Benjamin Wilder, Meng Yu, Kun Bai, Peng Liu. Technical Report: "NeuCloud: Enabling Privacy-preserving Monitoring in Cloud Computing." VCU CyberSecurity Lab. 2011.
3. Meng Yu, Peng Liu, and Wanyu Zang. "A Practical Model for Performance Evaluation of Attack Recovery Systems – PEARS". Technical Report TR-S2-03-05, Cyber Security Group, 2003
4. Meng Yu, Peng Liu, and Wanyu Zang. "A Practical Architecture for Distributed Intrusion Masking Database Systems", Technical Report, PSU-S2-2002-002, Penn State Cyber Security Group, 2002.

4.4.7 Theses

1. "Parallelizing Techniques of Object-Oriented Languages". Ph.D. dissertation. Department of Computer Sciences and Technology, Nanjing University, Nanjing, China, November, 2001. Supervisor: Prof. Zhongxiu Sun and Prof. Li Xie.
2. "Research on automatic proof-reading of Chinese text". M.S. thesis. Department of Computer Science, Northeastern University, Shenyang, China, March, 1998. Supervisor: Prof. Tianshun Yao.

4.5 Presentations and Talks

1. "Protection against Compromised Operating Systems on ARM Cortex-A Architecture". The Center for Education and Research in Information Assurance and Security (CERIAS) of Purdue University. West Lafayette, IN. February, 2019. Direct link to Purdue CERIAS website
2. "Privacy in Cloud Computing". *ISC Industry Day Event: Mitigating Consequences of a Cyber Security Attack & Building the Human Firewall*. McLeen, VA. April 24, 2013.
3. "An Attack-Resilient Channel Assignment MAC Protocol". *The 12th International Conference on Network-Based Information Systems (NBiS'09)*, Indianapolis, IN. August. 2009.
4. "Database Isolation and Filtering against Data Corruption Attacks", *The proceedings of the 21th Annual Computer Security Applications Conference, 2007 (ACSAC'07)*, Miami, FL, 2007
5. "Decentralized Trust Management based on the Reputation of Information Sources". 7th New Jersey Universities Homeland Security Research Consortium Symposium. Rutgers University, New Jersey. November, 2006.
6. "Defensive Execution of Transactional Processes against Attacks". The 21th Annual Computer Security Applications Conference, 2005 (ACSAC'05), Tucson, AZ.
7. "Self Healing Workflows under Attacks", 5 minute talk, IEEE Symposium on Security and Privacy, 2005. Oakland, CA
8. "Multi-version based Attack Recovery of Workflow", at the Annual Computer Security Applications Conference, 2003. (ACSAC'03), Las Vegas, Dec, 2003
9. "Intrusion Masking for Distributed Atomic Operations", at The Cyber Security Lab, Pennsylvania State University, University Park, April, 2003
10. "JAPS-II: A Source to Source Parallelizing Compiler for Java". At the 2002 International Conference on Parallel and Distributed Processing Techniques and Applications (PDPTA'02), Las Vegas, June, 2002

4.6 Postdoctoral Scholar Advised

- Yan Yang, Ph.D. of Japan Advanced Institute of Science and Technology. Joined University of Maryland, College Park as a post-doctoral scholar in January, 2011.

4.7 Graduate Students Advised

4.7.1 Ph.D. Students

- Naiwei Liu, graduated in October, 2020. First employment at University Davenport.
- Jin Han, graduated in November, 2019, First employment at Samsung Research, Austin, Texas.
- Min Li, Ph.D. graduate in May, 2015. First employment at FireEye. CA, USA.
- David Jackson, Ph.D. graduate in June, 2015. First employment at FireEye. CA, USA.

- Wuqiong Pan, Ph.D. graduated in November, 2013. First employment at Institute of Information Engineering, Chinese Academy of Science.

4.7.2 Ph.D. Dissertation

I directed the following students.

- Jin Han, *Enhance security in cloud computing through virtual machine placement.*
- Naiwei Liu, *Cache-based attack and defense on ARM platform.*
- Min Li, *Privacy Protection on Cloud Computing*
- David Jackson, *Rogue Signal Threat on Trust-based Cooperative Spectrum Sensing in Cognitive Radio Networks*
- Wuqiong Pan, *Research on virtual machine security.*

I served the following Ph.D. advisory committees, not as the advisor.

- Andrew C Jung, On Relay Node Placement Problem for Survivable Wireless Sensor Networks. December, 2013
- Lan Wu, Exploring Hybrid SPM-Cache Architectures to Improve Performance and Energy Efficiency for Real-time Computing. December, 2013.
- Guanying Wu, Performance and Reliability Study and Exploration of NAND Flash-based Solid State Drives. June, 2013.
- Sharad Shandilya. Assessment and Prediction of Cardiovascular Status During Cardiac Arrest Through Machine Learning and Dynamical Time-Series Analysis. July, 2013
- Sardar Ansari, Motion Artifact Reduction in Impedance Plethysmography Signal. June, 2013
- Xuguang Qi, Image analysis of corrosion growth rate of Aluminium and Steel. May, 2013.
- Chentao Wu, Improve the Performance and Scalability of RAID-6 Systems Using Erasure Codes. November, 2012.
- Yiqiang Ding, WCET Optimizations and Architectural Support for Hard Real-Time Systems. November, 2012.
- Yurong Luo, The Severity of Stages Estimation During Hemorrhage Using Error Correcting Output Codes Method. August, 2012
- Ashwin Belle, A Physiological Signal Processing System for Optimal Engagement and Attention Detection. July, 2012.
- Jie Wu, Segmentation and Fracture Detection in CT Images for Traumatic Pelvic Injuries. April, 2012.

4.7.3 M.S. Thesis

I directed the following thesis work as the advisor.

- Yulong Zhang, Towards an incentive-compatible framework of secure cloud computing, May, 2012
- Yufeng Zhen, A Novel Spam Campaign in Online Social Networks. November, 2013.

I was in the advisory committee of following students.

- David Jackson, Exploiting and Protecting Sensor Trust in Cooperative Spectrum Sensing for Cognitive Radio Networks. April, 2013
- Qiang Wang, The Role of Zinc Particle Size and Loading in Cathodic Protection Efficiency. December, 2012.
- Yan Fang, Simulation, Measurement, and Image Analysis of Corrosion Initiation and Growth Rate of Alumium 2024 and Steel 304. August, 2011.

4.8 Other Activities

I have hosted the following visiting scholars in my research lab for collaborative research.

- Zhiyi Ma, Associate Professor, Peking University
- Shanchen Pang, Associate Professor and Associate Dean, Shandong University of Science and Technology
- Chengpo Mu, Associate Professor, Beijing Institute of Technology

Teaching Activities

Teaching and curriculum work has emphasized cybersecurity, secure systems, cloud computing, operating systems, computer architecture, graduate seminars, and interdisciplinary program development. The full course history is retained below to document both administrative curriculum leadership and long-term teaching breadth.

5.1 Curriculum Development

- A new B.A. in Music and Computing program at Roosevelt University.
- A new MS in Cybersecurity and Information Assurance program at Roosevelt University.
- A graduate-level course *Cloud Computing and Virtualization Security* at UTSA.
- An undergraduate-level course *Distributed System and Cloud Computing Security* at UTSA.
- A graduate-level course *Cloud Computing* with security emphasis was developed at Virginia Commonwealth University.
- Served as co-director of the M.S. in Computer and Information System Security and updated the curriculum of the program at Virginia Commonwealth University.
- A new concentration (with colleagues), *Security of Information Systems and Networks*, graduate program at Monmouth University.
  - *Fundamentals of Computer Security and Cryptography* (graduate level)
  - *Computer Security* (graduate level)
  - *Network Security* (graduate level)
  - *Database and Transactions Security* (graduate level)

5.2 Courses Taught

Courses at Governors State University

CPSC-4435 Secure Programming
CPSC-4535 Introduction To Unix Systems
CPSC-8985 Grad Seminar in CPSC
CPSC-8820 Planning Management Software Project

Courses at University of West Florida

CIS 2530 Introduction to Cybersecurity
CIS 4221 Ethical Hacking and Pent Test
CIS 5775 Cybersecurity Principles
COT 6935 Seminar in Cybersecurity

Courses at Roosevelt University

CST/CSIA 317 Operating Systems, every fall
CST455 Cloud computing and security, every spring

Courses at University of Texas at San Antonio

CS3853 Computer Architecture, fall, 2016
CS3743 Computer Organization, fall, 2015
CS6393 Cloud computing and virtualization security, spring, 2016

Courses at Virginia Commonwealth University

CMSC312 Operating System, spring 2011, 2012, 2013, 2014, and fall 2013
CMSC622 Operating System and Networks Security, fall 2010, 2011, 2012, and 2013
CMSC691 Cloud Computing, Spring 2013

Courses at Western Illinois University

CS400 Computer Organization, every semester since fall 2007
CS410 Operating Systems, every semester since fall 2007
CS470 Database Systems, spring 2009
CS560 Computer Architecture every fall of 2007, 2008, and 2009
CS590 Database and Transactions Security, Spring 2008

Courses at Monmouth University

CS528 Database and Transactions Security, Spring 2007
CS698 Network Security, Fall 2005
CS598 Computer Security, Fall 2004, Fall 2006
CS505 (SE-698, CS-438) Operating Systems, Summer, 2005, Fall 2005, Spring 2006, Fall 2006
CS509 Advanced Programming II, Fall 2004, Spring 2005, Fall 2005, Spring 2006
CS502 Math Foundation of Computer Science, Spring 2005

Courses at Pennsylvania State University

IST402 Network security, Spring 2004, Guest Lecturer
IST220 Networking and Communications, Spring 2004, Guest Lecturer

Undergraduate Courses at Nanjing University

Compiler principles — Spring 2000, Spring 2001,
Operating systems — Fall 2000
Unix and C — Spring 2000
Computer network — Fall 1999

Services

6.1 University Services

- Member of the university Enrollment, Marketing, Retention Working Group, Roosevelt University, 2022-2023.
- University web contents advisory committee, Roosevelt University, 2020-2023.
- Member of university senate, Roosevelt University, 2018-2023.
- University graduate council, Roosevelt University, 2018-2023.
- University undergraduate council, Roosevelt University, 2018-2023.
- Undergraduate Committee, College of Art and Science, Roosevelt University, 2018-2023.
- Chair of MS committee, Department of Computer Science, UTSA, 2015-2018.
- Faculty search committee, Department of Computer Science, UTSA, 2015, 2016, 2017.
- Graduate committee, Department of Computer Science, UTSA, 2015, 2016, 2017.
- Online program committee, Department of Computer Science, UTSA, 2015, 2016.
- Graduate director, Computer Science department, Virginia Commonwealth University, 2013-2014.
- Co-director, M.S. in Computer and Information System Security, joint program by School of Engineering and School of Business, Virginia Commonwealth University, 2010-2015.
- School of Engineering Promotion and Tenure Committee, Virginia Commonwealth University, 2013-2015.
- University Promotion and Tenure Committee, Virginia Commonwealth University. 2012-2013.
- Faculty search committee, English Language Program, 2013.
- Faculty search committee, Computer Science department, 2013.
- Graduate Committee, Department of Computer Science, Virginia Commonwealth University, 2010-2015.
- University Research Council, Department of Computer Science, Western Illinois University, 2008-2010.
- Undergraduate Committee, Department of Computer Science, Western Illinois University, 2007-2010.

- Graduate program co-director, Department of Computer Science, Monmouth University, 2006-2007.
- Departmental library coordinator, Department of Computer Science, Monmouth University, 2005-2007.
- Teaching Learning Technology Round table (TLTR) Committee, School of Science, Technology, and Engineering, 2004-2007
- Graduate Study Committee, Monmouth University, 2006-2007
- Governance Task Force Committee, Monmouth University, 2005-2007

6.2 Professional Activities

6.2.1 NSF Panelist

- CSGrad4US, 2022
- Secure and Trustworthy Cyberspace (SaTC), NSF, 2012, 2014, 2015, 2016, 2017
- Computer Systems Research (CSR), NSF, 2013
- Trusted Computing (TC), NSF, 2009
- Cyber Trust (CT), NSF, 2008

6.2.2 Conference and workshop organization

- The 27th International Conference on Computer Communications and Networks (ICCCN 2018) HOT Track Chair.
- Workshop on Privacy in the Electronic Society 2017, Dallas, Texas. Session Chair.
- The 27th Annual IFIP WG 11.3 Working Conference on Data and Applications Security and Privacy (DBSEC) 2013, Session chair.
- The 25th Annual IFIP WG 11.3 Working Conference on Data and Applications Security and Privacy (DBSEC) 2011, General Co-Chair
- Security in Emerging Wireless Communication and Networking Systems (SEWCN) Workshop 2009, Co-Chair
- International Workshop on Information Assurance in Distributed Systems (IADS) 2005, Co-Chair

6.2.3 Editorial Board

- Journal of Internet Services and Information Security (JISIS)
- Intelligent Automation & Soft Computing (IASC), Impact Factor (IF) 3.401

6.2.4 Program Committee Service

I have served on the Program Committee of the following conferences and workshops.

- CloudNet2022, IEEE CNS 2022, WISA 2022, ICICS 2022, SSS-22
- CloudNet2021, IEEE CNS 2021, IEEE MASS 2021, IEEE SPC 2021, MobiSec 2021, ICICS 2021, ICCCN 2021

- CloudNet2020, 3ICT2020, ICNC'20 MCVC, ICNC'20, ISA, ICNC'20 CIS, IEEE CNS 2020, IEEE SPC 2020, IEEE WCNC 2020, SSCC 2020, WISA 2020, ICDCS 2020, ICMC 2020
- CloudNet2019, 3ICT'19, ICNC'19 CIS, ICNC'19 ISA, ICNC'19 MCVC, IEEE CNS 2019, IEEE MASS 2019, IEEE MENACOMM'19. IEEE SPC 2019, SSCC 2019, DSC 2019, WEPS2019, WISA 2019, CODASPY 2019
- CloudNet2018, ICNC'18 CIS, ICNC'18 ISA, ICNC'18 MCVC, IEEE CNS 2018, IEEE MASS'18, IEEE CNS 2018, SSCC 2018, SecureCOMM 2018, GPC-2018, ICCCN 2018
- ICISS 2017, WPES, 2017, MIST 2017, ATCI 2017, ICISS 2017, AsiaCCS-SCC 2017, ICMC 2017, ACN-2017, IEEE TENSYMP 2017, DBSec 2017, ISPA 2017, ESORICS 2017, ICMC 2017
- MIST 2016, WPES 2016, WISTP 2016 CANS 2016, IEEE TrustCom 2016, SCC 2016
- MIST 2015
- European Symposium on Research in Computer Security (ESORICS) 2014, 2015, 2016, 2017
- DBSEC'14,15,16
- CoNeD 2013, DBSEC'13, NAS'13, MIST'13, WPES'13
- CSOSN'12, DBSEC'12, ESTEL-SEC2012, NAS'12
- DBSEC'11, Inscrypt'11, ICCCN 2011, GCâ11 NGN, PETSE 2011, ICDT 2011
- DBSEC'10, Inscrypt'10, MIST'10, GC'10 NGN, ICDT'10, ARES'10
- SEWCN'09, IPCCC'09, WIDA'09, SECRYPT 2009, ARES 2009, IRI 2009
- DBSec 2008, ARES 2008, SSN 2008, IEEE ICNSC 2008, ICDT2008
- SECRYPT 2007, ARES 2007, ISDPE 2007, ATC 2007
- IRI 2006, ICDT 2006, SESYS 2006, SECRYPT 2006, DBSec 2006
- SecUbiq 2005

6.2.5 Reviewer for conferences and journals

- Journal of Computer Security
- ACM Transactions on Information and System Security (TISSSEC)
- IEEE Transactions on Dependable and Secure Computing (TDSC)
- IEEE Transaction on Knowledge and Data Engineering (TKDE)
- IET Information Security
- IEEE Transactions on Systems, Man and Cybernetics (TSMC)
- Security and Communication Networks
- International Journal of Intelligent and Control Systems
- Journal of Digital Library.
- Journal of Software (in Chinese).
- Journal of Computer Research and Development (in Chinese).

- ICNSC'05, ICNSC'06,
- Annual Computer Security Applications Conference (ACSAC'04, ACSAC'05)
- ITCC'05, Globecom'05, SecureComm'05, ESORICS'05, ICNSC'05, ICNSC'06, SecUbiq'05 ITCC'05
- ACM Conference on Computer and Communications Security (CCS'02, CCS'03).
- IFIP International Information Security Conference (SEC'04).
- IFIP WG 11.3 on Data and Application Security (DBSec'03).

Other Achievements

7.1 Projects

I participated in the following projects as principal personnel (NOT as PI).

1. Securing space platform. Sandia National Lab. Consultant through Purdue University. 2019-Present.
2. The work on workflow recovery is supported in part by DARPA/AFRL F20602-02-1-0216, Aug, 2002-Feb, 2003. I proposed fundamental theories for attack recovery of workflows. My theories are dependency relation based. I built a set of mathematical models to evaluate their performance and integrity levels. I have also built a prototype system to do extensive experiments. The theoretical results are well confirmed by our prototype system. Both single version and multiple version based recovery are practical according to our evaluation.
3. The work on intrusion tolerance is supported in part by NSF CCR-TC-0233324, and by Department of Energy Early Career PI Award. In this work, I formally specified a set of building blocks by the state machine model for distributed systems. We combined these building blocks to intrusion masking models that can provide non-degradation service in the face of intrusions. We also proposed protocols to implement the building blocks. Finally, we evaluated our protocols to ensure that they are practical. Our techniques can be applied to build intrusion masking atomic distributed operations.
4. Security extension to Linux. Supported by the National Hi-Tech Research and Development Program of China (863 Project). Contract Number 863-301-6-4. 2000,8-2001,3.
5. Development of Security Operating System based on Linux. Supported by the National Hi-Tech Research and Development Program of China (863 Project). Contract Number 863-306-ZD12-14-3. 2000,8-2001,1
6. Security Techniques Research in National Supercomputing Environment. Supported by the National Hi-Tech Research and Development Program of China (863 Project) as a sub project of 863 Key Project "Grid Software". 2000,8-2001,3
7. Research on Security Operating System based on Linux. Supported by Ministry of Education Young Teacher foundation. 2000,8-2001,10

   Work 3,4,5 and 6 developed a secure operating system. Our secure operating system passed evaluation with TCSEC B1 level by Ministry of Public Security in Feb. 2001. It is the second B1 level and the highest security level commercial operating system in China.
8. Parallelizing compiler of Java. Supported in part by the National Hi-Tech Research and Development Program of China (863 Project) and National Climber Project. 1998,4-2000,7. This work developed a compiler for Java that transforms sequential Java programs into parallel Java programs running on a cluster or multi-processor computers.

7.2 Other Honors and Awards

1. “Science and Technology Achievement”, China Ministry of Education. This was issued to our research group at Department of Computer Sciences and Technology, Nanjing University, China, 2001
2. “Excellent Scholar” The fifth national advanced training course for doctors and professors, by National 863-306 Committee, Beijing, China, Aug. 2001.
3. “Excellent achievement of science and techniques”, Science Committee of Shenyang, China, 1991. (A Computer real-time monitor system of slop pump)

Last updated: June 2026