Wenliang (Kevin) Du's Curriculum Vitae

Current Address: 4-206 Sci-Tech Building, Syracuse, NY 13244, USA
+1 315 443-9180, wedu@syr.edu, http://www.cis.syr.edu/∼wedu/

Research Areas System Security and Cybersecurity Education.

Education

Purdue University West Lafayette, IN
Ph.D. in Computer Science August 2001
M.S. in Computer Science December 1999
Research Area: Computer and Information Security
Ph.D. Thesis: A Study of Several Specific Secure Two-Party Computation Problems
Advisors: Dr. Mikhail J. Atallah and Dr. Eugene H. Spafford

Business School, Purdue University West Lafayette, IN
Certificate from Applied Management Principles Program May 2000

Florida International University Miami, FL
M.S. in Computer Science June 1996
Research Area: Software Engineering
Advisor: Dr. Yi Deng

University of Science and Technology of China Hefei, China
B.S. in Computer Science July 1993
Advisor: Dr. Chih-Sung Tang

Experience

Syracuse University, Syracuse, NY *Professor*
Department of Electrical Engineering & **June 2012 – Present**
Computer Science (EECS) *Associate Professor*
July 2007 – May 2012
Assistant Professor
Aug. 2001 – June 2007
Teaching, advising, and conducting original research in the areas related to computer, information, and network security.

Purdue University, West Lafayette, IN *Research Assistant*
Department of Computer Science & CERIAS **Aug. 1996 – July 2001**
Conducting research in computer and information security areas in the Center of Education and Research in Information Assurance and Security (CERIAS), Purdue University.

Microsoft *Internship*
Redmond, WA. **May 1998 – Nov. 1998**
Analyze the security relevance of the Registry in Windows NT 4.0.

Awards, Patents, and Recognitions

- 2022: Elevated to IEEE Fellow for contributions to cybersecurity education and research.
- 2022 IEEE Region 1 Technological Innovation (Academic) Award.
- **Test-of-Time Awards:**
  - 2021 ACSAC Test-of-Time Award.
  - 2013 ACM CCS Test-of-Time Award, which recognizes papers from CCS ten years prior (CCS 2003) that have had the greatest impact on security research and practice over the past decade.

- **Citations:** The total number of citations of my research papers is **17,578** (source: Google Scholar). H-index: 57, i10-index: 100.
- The hands-on labs (SEED labs) that I developed for security education have been used by over **1090** universities and colleges in more than 80 countries.
- My book (Computer & Internet Security: A Hands-on Approach, 1st to 3rd edition), has been adopted by **273** universities and colleges worldwide.
- Have organized 14 workshops in the last 6 years. Have trained over 800 professors.
- 2019 Meredith Professorship for Teaching Excellence. This is a life-time title and is the highest teaching award at Syracuse University.
- 2017 Academic Leadership award from The 21st Colloquium for Information System Security Education.
- 2014 Dean's Award for Excellence in Engineering Education.
- 2013 Faculty Excellence Award from L.C.Smith College of Engineering and Computer Science (including a $20,000 research fund).
- Best Paper Award in the 5th Annual Symposium on Information Assurance (ASIA '10). June 16-17, 2010, Albany, New York.
- Best Paper Award in The 11th Pacific-Asia Conference on Knowledge Discovery and Data Mining (PAKDD-07), May 22-25, 2007, Nanjing, China.
- Best Paper Award in The 19th IEEE International Parallel & Distributed Processing Symposium (IPDPS 2005), April 4-8, 2005, Denver, Colorado.
- Presidential Fellowship (1994-1996), Florida International University.
- Guo Mo-ruo Award (1992), University of Science & Technology of China.
- First-class prize winner (the 7th place in the province) in the National High-school Mathematics Contests (1988).
- First-class prize winner (the 5th place in the province) in the National High-school Mathematics Contests (1987)

Fundings

Serving as PI

1. Building an Internet Emulator for Cybersecurity Education.
   NSF-SaTC, 10/2022 - 09/2025, $399,197, PI.
2. Expanding TrustZone: Enabling Mobile Apps to Transparently Leverage TrustZone for Attestation and Data Protection.
   NSF, 08/2017 - 08/2020, $497,296, PI.
3. Spreading SEEDs: Large-Scale Dissemination of Hands-on Labs for Security Education.
   NSF, 09/2014 - 08/2018, $863,385, PI.
4. Develop Fine-Grained Access Control for Third-Party Components in Mobile Systems.
   NSF-SaTC, 08/2013 - 07/2017, $532,362, PI.
5. Collaborative: Bolstering Security Education through Transiting Research on Browser Security.
   NSF-SaTC, 09/2013 - 09/2015, $89,878, PI.
6. Security-Enhanced WebView for Android System.
   Google Research Award, 12/2011 - 12/2012, $49,387, PI.
7. To Configure or to Implement, That is the Access Control Question for Web Applications.
   NSF-TC (Trustworthy Computing), 09/2010 - 08/2014, $506,470, PI.
8. SEED: Developing Instructional Laboratories for Computer Security Education.
   NSF-CCLI (Type II), 01/2007-12/2011, $451,682, PI.
9. Collaborative Research: Trustworthy and Resilient Location Discovery in Wireless Sensor Networks.
   NSF CyberTrust, 9/2004-8/2007, $150,000, PI.

10. Collaborative Research: ITR: Distributed Data Mining to Protect Information Privacy.
NSF-ITR, 8/2003-7/2006, $140,418, PI.
11. Private Prediction using Selective Models.
NSF-ITR, 9/2002-8/2005, $220,000, PI.
12. Designing Laboratory Materials for Computer System Security Courses Using Minix Instructional Operating System.
NSF-CCLI (Type I), 01/2003-12/2005, $74,984, PI.
13. Efficient and Resilient Key Management for Wireless Sensor Networks.
Army Research Office (ARO), 5/2005-4/2008, $360,000, PI.
14. VINE: Using VIrtual Network Environment for Computer and Network Security Courses.
University Vision Fund, 1/2003-12/2003, $5,000, PI.

Serving as co-PI

14. Creating Educational Foundations for Assured Systems.
NSF-TUES, Susan Older (PI), 09/2013 - 08/2015. $200,000.
15. Exploiting Network Dynamics for Secret Key Generation.
NSF-TC, Yingbin Liang (PI), 09/2011 - 08/2014. $300,084.
16. Data Fusion and Visualization.
JPMorgan Chase, Jae Oh (PI), Howard Blair (co-PI), 05/2010 - 12/2011, $500,000.
17. Identity Management.
JPMorgan Chase, Joon Park (PI), 01/2008 - 12/2008, $150,000
18. Multi-Institutional Curriculum Development and Delivery to Create the New Smart Grid Workforce.
Department of Energy, Chilukuri K Mohan (PI), $2,500,000.
19. Cyber Superiority for Air Force Combatant Commanders: Integrated Air/Space/C2/Cyber Dynamic Spectrum Exploitation for Enhanced Situational Awareness-Phase II.
Air Force Office of Scientific Research through ANDRO Computational Solutions, LLC.
Pramod Varshney (PI), 2/11/2011 - 9/29/2012. $285,000.
20. Cyber Superiority for Air Force Combatant Commanders: Integrated Air/Space/C2/Cyber Dynamic Spectrum Exploitation for Enhanced Situational Awareness-Phase I.
Air Force Office of Scientific Research through ANDRO Computational Solutions, LLC.
Pramod Varshney (PI), 08/2009 - 5/2010, $40,070.

Publications

Book

1. Wenliang Du. **Computer Security: A Hands-on Approach**, 3rd edition. Independently Published. ISBN: 978-17330039-5-7. May 2022.
2. Wenliang Du. **Internet Security: A Hands-on Approach**, 3rd edition. Independently Published. ISBN: 978-1-7330039-6-4. May 2022.
3. Wenliang Du. **Computer Security: A Hands-on Approach, Chinese Version**. Published by Chinese Higher Education Press in April 2020.

Journal

4. Kapil M. Borle, Biao Chen, and Wenliang Du. **Physical Layer Spectrum Usage Authentication In Cognitive Radio: Analysis and Implementation**. In *IEEE Transactions on Information Forensics & Security*, Vol. 10, No. 10, October 2015.
5. Kaiqi Xiong, Ronghua Wang, Wenliang Du, and Peng Ning. **Containing Bogus Packet Insertion Attacks for Broadcast Authentication in Sensor Networks**. In *ACM Transactions on Sensor Networks*, Volume 8 Issue 3, July 2012.

6. Wenliang Du, **The SEED Project: Providing Hands-on Lab Exercises for Computer Security Education**. To Appear in *IEEE Security and Privacy Magazine*, September/October, 2011. This is an invited paper.
7. Huseyin Polat, Wenliang Du, Sahin Renckes, and Yusuf Oysal. **Private predictions on hidden Markov models**. In *Artificial Intelligence Review*, Volume 34 Issue 1, June 2010.
8. Ronghua Wang, Wenliang Du, Xiaogang Liu, and Peng Ning. **ShortPK: A Short-Term Public Key Scheme for Broadcast Authentication in Sensor Networks**. In *ACM Transactions on Sensor Networks*, Vol. 6, No. 1, Article 9, pages 1–29, December 2009.
9. Wenliang Du and Ronghua Wang. **SEED: A Suite of Instructional Laboratories for Computer Security Education**. In *The ACM Journal on Educational Resources in Computing (JERIC)*, Volume 8, Issue 1, March 2008.
10. Donggang Liu, Peng Ning, and Wenliang Du. **Group-Based Key Pre-Distribution in Wireless Sensor Networks**. In *ACM Transactions on Sensor Networks (TOSN)*, Vol. 4, No. 2, pages 11:1–11:30, March 2008.
11. Donggang Liu, Peng Ning, An Liu, Cliff Wang, Wenliang Du. **Attack-Resistant Location Estimation in Wireless Sensor Networks**. In *ACM Transactions in Information and Systems Security (TISSEC)*, 2008.
12. Peng Ning, An Liu, and Wenliang Du. **Mitigating DoS Attacks against Broadcast Authentication in Wireless Sensor Networks**. In *The ACM Transactions on Sensor Networks (TOSN)*, Vol. 4, No. 1, February 2008.
13. Huseyin Polat and Wenliang Du. **Privacy-Preserving Top-N Recommendation on Distributed Data**. In the *Journal of the American Society for Information Science and Technology*, Volume 59, Number 7, May 2008.
14. Shigang Chen, Yong Tang, and Wenliang Du. **Stateful DDoS Attacks and Targeted Filtering**. Accepted by *Journal of Network and Computer Applications*, Special Issue on Distributed Denial of Service and Intrusion Detection, vol. 30, issue 3, August 2007.
15. Wenliang Du, Jing Deng, Yunghsiang S. Han, and Pramod Varshney. **A Key Predistribution Scheme for Sensor Networks Using Deployment Knowledge**. In *IEEE Transactions on Dependable and Secure Computing*, Volume 3, Number 2, January-March 2006. Pages 62-77.
16. Wenliang Du, Lei Fang and Peng Ning. **LAD: Localization Anomaly Detection for Wireless Sensor Networks**. In *The Journal of Parallel and Distributed Computing (JPDC)*, Volume 66, Issue 7, July 2006. Pages 874-886.
17. Wenliang Du, Mingdong Shang, and Haizhi Xu. **A Novel Approach for Computer Security Education using Minix Instructional Operating System**. In *Computer & Security*, Volume 25, Issue 3, 2006. Pages 190-200.
18. Wenliang Du, Jing Deng, Yunghsiang S. Han, Pramod Varshney, Jonathan Katz, and Aram Khalili. **A Pairwise Key Pre-distribution Scheme for Wireless Sensor Networks**. In *The ACM Transactions on Information and System Security (TISSEC)*, Volume 8, Issue 2, May 2005. Pages 228-258.
19. Ninghui Li, Wenliang Du, and Dan Boneh. **Oblivious Signature-based Envelope**, In *Distributed Computing*, Vol. 17, No. 4, 2005. Pages 293-302. Publisher: Springer-Verlag.
20. Huseyin Polat and Wenliang Du. **Privacy-Preserving Collaborative Filtering**. In the *International Journal of Electronic Commerce (IJEC)*, pages 9-35. Volume 9, Number 4, Summer 2005.
21. Wenliang Du and Aditya P. Mathur. **Testing for Software Vulnerability Using Environment Perturbation**. In *Quality and Reliability Engineering International*, Volume 18 Issue 3, 2002. Special Issue: Secure, Reliable Computer and Network Systems. Page 261-272.

Refereed Conference & Workshop Proceedings

23. Wenliang Du, Honghao Zeng, and Kyungrok Won. **SEED Emulator: An Internet Emulator for Research and Education**. In *Proceedings of HotNets 2022: Twenty-First ACM Workshop on Hot Topics in Networks*, November 14 - 15, 2022, Austin, Texas, USA

24. Amit Ahlawat and Wenliang Du. **TruzCall: Secure VoIP Calling on Android using ARM TrustZone**. In *Proceedings of MobiSecServ 2020 Internatinal conference*, February 22 - 23, 2020, Miami, FL, USA.

25. Kailiang Ying, Priyank Thavai, and Wenliang Du. **TruZ-View: Developing TrustZone User Interface for Mobile OS Using Delegation Integration Model**. In *Proceedings of the 9th ACM Conference on Data and Application Security and Privacy*, March 25 - 27, 2019, Richardson, TX, USA.

26. Kailiang Ying, Amit Ahlawat, Bilal Alsharifi, Yuexin Jiang, Priyank Thavai, and Wenliang Du. **TruZ-Droid: Integrating TrustZone with Mobile Operating System**. In *Proceedings of The 16th ACM International Conference on Mobile Systems, Applications, and Services (MobiSys 2018)*. June 10 - 15, 2018. Munich, Germany.

27. Carter Yagemann and Wenliang Du. Intentio Ex Machina: **Android Intent Access Control via an Extensible Application Hook**. In *Proceedings of the 21st European Symposium on Research in Computer Security (ESORICS'16)*. Heraklion, Crete, Greece. September 26-30, 2016.

28. Xiao Zhang, Yousra Aafer, Kailiang Ying and Wenliang Du. **Hey, You, Get Off of My Image: Detecting Data Residue in Android Images**. In *Proceedings of the 21st European Symposium on Research in Computer Security (ESORICS'16)*. Heraklion, Crete, Greece. September 26-30, 2016.

29. Yousra Aafer, Xiao Zhang, and Wenliang Du. **Harvesting Inconsistent Security Configurations in Custom Android ROMs via Differential Analysis**. In *Proceedings of the 25th USENIX Security Symposium (USENIX Security'16)*, Austin, Texas, USA. August 10-12, 2016.

30. Xiao Zhang, Kailiang Ying, Yousra Aafer, Zhenshen Qiu, and Wenliang Du. **Life after App Uninstallation: Are the Data Still Alive? Data Residue Attacks on Android**. In *Proceedings of the Network and Distributed System Security Symposium (NDSS)*, San Diego, California, USA. February 21-24, 2016.

31. (Yousra Aafer, Nan Zhang) co-first author, Zhongwen Zhang, Xiao Zhang, Kai Chen, XiaoFeng Wang, Xiaoyong Zhou, Wenliang Du, and Michael Grace. **Hare Hunting in the Wild Android: A Study on the Threat of Hanging Attribute References**. In *Proceedings of the 22nd ACM Conference on Computer and Communications Security (CCS)*, Denver, Colorado, USA. October 12-16, 2015.

32. Paul Ratazzi, Ashok Bommisetti, Nian Ji, and Wenliang Du. **PINPOINT: Efficient and Effective Resource Isolation for Mobile Security and Privacy**. In *Proceedings of the Mobile Security Technologies (MoST) workshop*, May 21, 2015.

33. Xing Jin, Xunchao Hu, Kailiang Ying, Wenliang Du, Heng Yin and Gautam Nagesh Peri. **Code Injection Attacks on HTML5-based Mobile Apps: Characterization, Detection and Mitigation**. In *Proceedings of the 21st ACM Conference on Computer and Communications Security (CCS)*, Scottsdale, Arizona, USA. November 3 - 7, 2014.

34. Xing Jin, Tongbo Luo, Derek G. Tsui, and Wenliang Du. **Code Injection Attacks on HTML5-based Mobile Apps**. In *Proceedings of the Mobile Security Technologies (MoST) workshop*, May 16, 2014.

35. Paul Ratazzi, Yousra Aafer, Amit Ahlawat, Hao Hao, Yifei Wang, and Wenliang Du. **A Systematic Security Evaluation of Android's Multi-User Framework**. In *Proceedings of the Mobile Security Technologies (MoST) workshop*, May 16, 2014.

36. Xiao Zhang and Wenliang Du. **Attacks on Android Clipboard**. In *Proceedings of the 11th Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA)*, Egham, UK. July 10-11, 2014.

37. Yifei Wang, Srinivas Hariharan, Chenxi Zhao, Jiaming Liu, Wenliang Du. **Compac: Enforce Component-Level Access Control in Android**. In *Proceedings of the 4th ACM Conference on Data and Application Security and Privacy (CODASPY)*. San Antonio, TX, USA. March 3-5, 2014.

38. Xiao Zhang, Amit Ahlawat, and Wenliang Du. **AFrame: Isolating Advertisements from Mobile Applications in Android**. In *Proceedings of the 29th Annual Computer Security Applications Conference (ACSAC)*, New Orleans, Louisiana, USA. December 9-13, 2013.

39. Xing Jin, Lusha Wang, Tongbo Luo, and Wenliang Du. **Fine-Grained Access Control for HTML5-Based Mobile Applications in Android**. In *Proceedings of the 16th Information Security Conference*, Dallas, Texas. November 13-15, 2013.

40. Yousra Aafer, Wenliang Du, and Heng Yin. **DroidAPIMiner: Mining API-Level Features for Robust Malware Detection in Android**. In *Proceedings of the 9th International Conference on Security and Privacy in Communication Networks (SecureComm)*. September 25-27, 2013 Sydney, Australia.

41. Tongbo Luo, Xing Jin, and Wenliang Du. **Mediums: Visual Integrity Preserving Framework**. In *Proceedings of the 3rd ACM Conference on Data and Application Security and Privacy (CODASPY)*, Feb 18-20, 2013. San Antonio, TX, USA.

42. Hao Hao, Vicky Singh and Wenliang Du. **On the Effectiveness of API-Level Access Control Using Bytecode Rewriting in Android**. In *Proceedings of the 8th ACM Symposium on Information, Computer and Communications Security*, May 7-10 2013.

43. Kapil M. Borle, Biao Chen, and Wenliang Du, **A Physical Layer Authentication Scheme for Countering Primary User Emulation Attack**. In *Proceedings of the 38th International Conference on Acoustics, Speech, and Signal (ICASSP)*. Vancouver, Canada, on May 26 - 31, 2013.

44. Tongbo Luo, Xing Jin, Ajai Ananthanarayana, and Wenliang Du. **Touchjacking Attacks on Web in Android, iOS, and Windows Phone**. In *Proceedings of the 5th International Symposium on Foundations & Practice of Security*, October 25-26, 2012.

45. Xi Tan, Wenliang Du, Tongbo Luo, and Karthick Soundararaj. **Scuta: A Server-Side Access Control System for Web Applications**. In *Proceedings of the 17th ACM SACMAT*, June 20-22, 2012, Newark, USA.

46. Tongbo Luo, Hao Hao, Wenliang Du, Yifei Wang, and Heng Yin. **Attacks on WebView in the Android System**. In *Proceedings of the Annual Computer Security Applications Conference (ACSAC)*, Orando, Florida. December 5 – 9, 2011.

47. Wenliang Du, Karthick Jayaraman, Xi Tan, Tongbo Luo and Steve Chapin. **Position Paper: Why Are There So Many Vulnerabilities in Web Applications?**. To Appear in *Proceedings of the New Security Paradigms Workshop (NSPW'11)*. Marin County, CA, USA. September 12 – 15, 2011.

48. Lifeng Lai, Yingbin Liang, and Wenliang Du. **PHY-Based Cooperative Key Generation in Wireless Networks**. To appear in *Proceedings of the 49th Annual Allerton Conference on Communication, Control, and Computing*. Monticello, Illinois. September 28 – 30, 2011.

49. Lifeng Lai, Yingbin Liang, Wenliang Du, and Shlomo Shamai. **Secret Sharing via Noisy Broadcast Channels**. In *Proceedings of the 2011 IEEE International Symposium on Information Theory*. Saint-Petersburg, Russia. July 31 – August 5, 2011.

50. Wenliang Du, Xi Tan, Tongbo Luo, Karthick Jayaraman, and Zutao Zhu. **Re-designing the Web's Access Control System**. In *Proceedings of the 25th Annual WG 11.3 Conference on Data and Applications Security and Privacy (DBSec'11)*, Richmond, Virginia USA. July 11-13, 2011.

51. Tongbo Luo and Wenliang Du. **Contego: Capability-Based Access Control for Web Browsers**. In *Proceedings of the 4th International Conference on Trust and Trustworthy Computing*, Pittsburgh, PA, June 22-25, 2011.

52. Xi Tan, Kapil Borle, Wenliang Du and Biao Chen. **Cryptographic Link Signatures for Spectrum Usage Authentication in Cognitive Radio**. In *ACM Conference on Wireless Network Security*, Hamburg, Germany, June 15-17, 2011.

53. Karthick Jayaraman, Wenliang Du, Balamurugan Rajagopalan, and Steve J. Chapin. **Escudo: A Fine-grained Protection Model for Web Browsers**. In *Proceedings of The 30th International Conference on Distributed Computing Systems (ICDCS)*, Genoa, Italy, June 21-25, 2010. (Acceptance ratio 14.4% = 84/585).

54. Wenliang Du, Karthick Jayaraman, and Noreen B. Gaubatz. **Enhancing Security Education with Hands-on Laboratory Exercises**. In *Proceedings of the 5th Annual Symposium on Information Assurance (ASIA '10)*. June 16-17, 2010, Albany, New York. **Best Paper Award**.

55. Zutao Zhu and Wenliang Du. **Understanding Privacy Risk of Publishing Decision Trees**. In *Proceedings of the 24th Annual IFIP WG 11.3 Working Conference on Data and Applications Security (DBSec 2010)*. Rome, Italy. June 21-23, 2010.

56. Guan Wang, Tongbo Luo, Michael Goodrich, Wenliang Du, and Zutao Zhu. **Bureaucratic Protocols for Secure Two-Party Sorting, Selection, and Permuting**. In *Proceedings of the ACM Symposium on Information, Computer and Communications Security*. Beijing, China, April 13-16, 2010. (Acceptance ratio: 15% = 25/166).

57. Zutao Zhu and Wenliang Du. **K-anonymous Association Rule Hiding** (short paper). In *Proceedings of the ACM Symposium on Information, Computer and Communications Security*. Beijing, China, April 13-16, 2010.

58. Wenliang Du, David Eppstein, Michael Goodrich and George Lueker. **On the Approximability of Geometric and Geographic Generalization and the Min-Max Bin Covering Problem**. In *Proceedings of Algorithms and Data Structres Symposium (WADS)*, 21-23 Auguest, 2009. Banff Conference Centre, Banff, Alberta, Canada.

59. Zutao Zhu, Guan Wang, and Wenliang Du. **Deriving Private Information from Association Rule Mining Results**. In *Proceedings of The 25th IEEE International Conference on Data Engineering (ICDE)*, Shanghai, China, March 29 - April 4, 2009. (Acceptance ratio 16.8% = 93/554).

60. Wenliang Du, Zhouxuan Teng, and Zutao Zhu. **Privacy-MaxEnt: Integrating Background Knowledge in Privacy Quantification**. In *Proceedings of the* ACM SIGMOD Conference, June 9-12, 2008, Vancouver, Canada. (Acceptance ratio 17.9% = 78/435).

61. Guan Wang, Zutao Zhu, Wenliang Du, and Zhouxuan Teng. **Inference Analysis in Privacy-Preserving Data Re-publishing**. In *Proceedings of the 8th IEEE International Conference on Data Mining (ICDM)*, Pisa, Italy, Dec. 15-19, 2008. (Acceptance ratio: 20% = 144/724).

62. Zhengli Huang and Wenliang Du. **OptRR: Optimizing Randomized Response Schemes for Privacy-Preserving Data Mining**. In Proceedings of the *24th IEEE International Conference on Data Engineering (ICDE)*, April 7-12, 2008, Cancun, Mexico. Full paper with 15-minute presentation (Total submission is 617, acceptance ratio for full paper with 30-minute presentation is 12.1%, and acceptance ratio for full paper with 15-minute presentation is an additional 7.1%).

63. Sangwon Hyun, Peng Ning, An Liu, Wenliang Du, **Seluge: Secure and DoS-Resistant Code Dissemination in Wireless Sensor Networks**. In *Proceedings of the 7th International Conference on Information Processing in Sensor Networks*, St. Louis, USA. April 22-24, 2008. (Acceptance ratio: 23.8% = 30/126).

64. Wenliang Du, Zhouxuan Teng, and Ronghua Wang. **SEED: A Suite of Instructional Laboratories for Computer Security Education**. In Proceedings of SIGCSE Technical Symposium on Computer Science Education. March 7-10, 2007, Covington, Kentucky, USA. (Acceptance ratio 34% = 108/316).

65. Ronghua Wang, Wenliang Du, and Peng Ning. **Containing Denial-of-Service Attacks in Broadcast Authentication in Sensor Networks**. In Proceedings of *the Eighth ACM International Symposium on Mobile Ad Hoc Networking and Computing*

(MobiHoc), Montreal, Quebec, Canada. September 9-14, 2007. (Acceptance ratio 18.5% = 27/146).

66. Zhengli Huang, Wenliang Du, and Zhouxuan Teng. **Searching for Better Randomized Response Schemes for Privacy-Preserving Data Mining**. In the *11th European Conference on Principles and Practice of Knowledge Discovery in Databases (PKDD)*. Poster Paper. September 17 - 21, 2007. Warsaw, Poland.

67. Zhouxuan Teng and Wenliang Du. **A Hybrid Multi-Group Privacy Preserving Approach for Building Decision Trees**. In Proceedings of the Pacific-Asia Conference on Knowledge Discovery and Data Mining (PAKDD-07). May 22-25, 2007, Nanjing, China. (Best Paper Award among 730 submissions).

68. Abdulrahman Alarifi and Wenliang Du. **Diversifying Sensor Nodes to Improve Resilience Against Node Compromise**, Accepted by the 4th ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN'06).

69. Huseyin Polat and Wenliang Du. **Achieving Private Recommendations Using Randomized Response Techniques**. In *The 10th Pacific-Asia Conference on Knowledge Discovery and Data Mining (PAKDD 2006)*, April 9-12, 2006, Singapore. Pages 637–646. (Acceptance ratio 20% = 100/501).

70. Zhouxuan Teng and Wenliang Du. **Comparisons of K-Anonymization and Randomization Schemes Under Linking Attacks**. In Proceedings of The IEEE International Conference on Data Mining (ICDM) (short paper). December 18-22, 2006, Hong Kong. (Acceptance ratio: 20% of 800).

71. Huseyin Polat and Wenliang Du. **Achieving Private Recommendations Using Randomized Response Techniques**. Accepted by *The 10th Pacific-Asia Conference on Knowledge Discovery and Data Mining (PAKDD 2006)*, April 9-12, 2006, Singapore. Pages 637–646. (Acceptance ratio 20% =100/501).

72. Zhengli Huang, Wenliang Du, and Biao Chen. **Deriving Private Information from Randomized Data**. In Proceedings of the ACM SIGMOD Conference, June 14-16, 2005, Baltimore, Maryland, USA. Pages 37-48 (Acceptance ratio 15.3% = 66/431)

73. Wenliang Du, Ronghua Wang, and Peng Ning. **An Efficient Scheme for Authenticating Public Keys in Sensor Networks**. In Proceedings of The 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc), May 25-28, 2005. Urbana-Champaign, Illinois, USA. Pages 58-67. (Acceptance ratio 14.2% = 40/281)

74. Lei Fang, Wenliang Du and Peng Ning. **A Beacon-Less Location Discovery Scheme for Wireless Sensor Networks**. In Proceedings of the IEEE INFOCOM'05, March 13-17, 2005, Miami, FL, USA. (Acceptance ratio 17.2% = 244/1419).

75. Wenliang Du, Lei Fang and Peng Ning. **LAD: Localization Anomaly Detection for Wireless Sensor Networks**. In the 19th International Parallel and Distributed Processing Symposium (IPDPS). **Best Paper Award** in the Algorithm track. April 4-8, 2005, Denver, Colorado, USA. (Acceptance ratio is 34.3% = 116/338).

76. Donggang Liu, Peng Ning, Wenliang Du, **Group-Based Key Pre-Distribution in Wireless Sensor Networks**, In Proceedings of 2005 ACM Workshop on Wireless Security (WiSe), September 2005. Pages 11 - 20.

77. Donggang Liu, Peng Ning and Wenliang Du. **Attack-Resistant Location Estimation in Sensor Networks** In Proceedings of The Fourth International Conference on Information Processing in Sensor Networks, 2005. Pages 99-106 (Acceptance ratio is 20.7% = 44/213).

78. Donggang Liu, Peng Ning and Wenliang Du. **Detecting Malicious Beacon Nodes for Secure Location Discovery in Wireless Sensor Networks**. In Proceedings of The 25th International Conference on Distributed Computing Systems (ICDCS), 2005. Pages 609-619. (Acceptance ratio 13.8% = 75/543).

79. Huseyin Polat and Wenliang Du. **Privacy-Preserving Top-N Recommendation on Horizontally Partitioned Data**. In *Proceedings of the IEEE/WIC/ACM International*

Conference on Web Intelligence (WI), September 19-22, 2005, France. Pages 725–731 (Acceptance ratio 18% of 328 submissions).

80. Huseyin Polat and Wenliang Du. **Privacy-Preserving Collaborative Filtering on Vertically Partitioned Data**. In *Proceedings of the 9th European Conference on Principles and Practice of Knowledge Discovery in Databases (PKDD)* (short paper). Porto, Portugal, October 3-7, 2005. Pages 651- 658.

81. Huseyin Polat and Wenliang Du. **SVD-based Collaborative Filtering with Privacy**. In The 20th ACM Symposium on Applied Computing, Track on E-commerce Technologies. Santa Fe, New Mexico, USA. March 13-17, 2005. Pages 791-795.

82. Wenliang Du and Michael T. Goodrich. **Searching for High-Value Rare Events with Uncheatable Grid Computing**. In *Applied Cryptography and Network Security (ACNS) Conference*, June 7-10, 2005. New York City, New York, USA. Pages 122-137 (Acceptance ratio 22.4% = 35/156).

83. Haizhi Xu, Wenliang Du, and Steve J. Chapin. **Context Sensitive Anomaly Monitoring of Process Control Flow to Detect Mimicry Attacks and Impossible Paths**. In RAID: Seventh International Symposium on Recent Advances in Intrusion Detection. French Riviera, France. September 15-17, 2004, Pages 21-38 (Acceptance ratio 13.5% = 16/118).

84. Haizhi Xu, Steve J. Chapin, and Wenliang Du. **Detecting Exploit Code Execution in Loadable Kernel Modules**. In ACSAC'04: the 20th Annual Computer Security Applications Conference. Tucson, Arizona, USA. December 6-10, 2004, Pages 101-110 (Acceptance ratio 26.1% = 35/134).

85. Wenliang Du, Jing Deng, Yunghsiang S. Han, Shigang Chen and Pramod Varshney. **A Key Management Scheme for Wireless Sensor Networks Using Deployment Knowledge**. In Proceedings of the *IEEE Infocom 2004*. (Acceptance Ratio: 18.4% = 261/1420)

86. Wenliang Du, Jing Jia, Manish Mangal and Mummoorthy Murugesan. **Uncheatable Grid Computing**. In *The 24th International Conference On Distributed Computing Systems (ICDCS 2004)*. Pages 4-11 (Acceptance Ratio: 17.7% = 84/475).

87. Wenliang Du, Yunghsiang S. Han and Shigang Chen. **Privacy-Preserving Multivariate Statistical Analysis: Linear Regression and Classification**. In Proceedings of the *2004 SIAM International Conference on Data Mining*, Lake Buena Vista, Florida, April 22-24, 2004. Page 222-233 (Acceptance Ratio 14.3% = 23/161).

88. Wenliang Du, Jing Deng, Yunghsiang S. Han, and Pramod Varshney. **A Pairwise Key Pre-distribution Scheme for Wireless Sensor Networks**. In *10th ACM Conference on Computer and Communications Security (CCS)*, Washington DC, October 27-31, 2003. Pages 42-51 (Acceptance Ratio: 13.9% = 35/252).

89. Ninghui Li, Wenliang Du, and Dan Boneh. **Oblivious Signature-based Envelope**. In *Proceedings of the 22nd ACM Symposium on Principles of Distributed Computing (PODC)*, Boston, Massachusetts. July 13-16, 2003. Page 182-189. **This paper is invited to submit to Springer-Verlag's journal Distributed Computing**. (Acceptance Ratio: 16.3% = 34/208).

90. Huseyin Polat and Wenliang Du. **Privacy-Preserving Collaborative Filtering**. In *Proceedings of the 3rd IEEE International Conference on Data Mining (ICDM)*, Melbourne, Florida, November 19-23, 2003. Pages 625-628 (Acceptance Ratio: 23.6% = 118/501).

91. Wenliang Du and Zhijun Zhan. **Using Randomized Response Techniques for Privacy-Preserving Data Mining**. In *Proceedings of the 9th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, Washington, DC, August 24 - 27, 2003. Pages 505-510 (Acceptance Ratio: 27.1% = 70/258).

92. Wenliang Du, Jing Deng, Yunghsiang S. Han, and Pramod Varshney. **A Witness-Based Approach For Data Fusion Assurance In Wireless Sensor Networks**.

In *Proceedings of IEEE 2003 Global Communications Conference (GLOBECOM)*, San Francisco, CA, USA. December 1-5, 2003. (Acceptance Ratio: 34.0% = 816/2400).

93. Mikhail J. Atallah, Florian Kerschbaum, and Wenliang Du. **Secure and Private Sequence Comparisions**. In *the ACM Workshop on Privacy in Electronic Society*, in association with *the 10th ACM Conference on Computer and Communications Security*, Washington DC, October 30, 2003. Pages 39-44 (Acceptance Ratio: 16/50)
94. Wenliang Du. **Developing an Instructional Operating System for Computer Security Education**. In *the 7th Colloquium for Information Systems Security Education (CISSE)*, Washington DC. June 3-5, 2003.
95. Wenliang Du and Zhijun Zhan. **Building Decision Tree Classifier on Private Data**. In *Workshop on Privacy, Security, and Data Mining at the 2002 IEEE International Conference on Data Mining (ICDM'02)*, Maebashi City, Japan. December 9, 2002.
96. Wenliang Du and Zhijun Zhan. **A Practical Approach to Solve Secure Multi-party Computation Problems**. In *New Security Paradigms Workshop*, Virginia Beach, Virginia, USA. September 23 - 26, 2002. (Acceptance Ratio: 14/40).
97. Wenliang Du and Mikhail J. Atallah. **Privacy-Preserving Cooperative Statistical Analysis**. In *2001 Annual Computer Security Applications Conference (ACSAC)*. New Orleans, Louisiana, USA. Pages 102-110. December 10-14, 2001.
98. Wenliang Du and Mikhail J. Atallah. **Secure Multi-Party Computation Problems and their Applications: A Review and Open Problems**. In *New Security Paradigms Workshop*, Cloudcroft, New Mexico, USA. Pages 11-20. September 11th - 13th, 2001.
99. Mikhail J. Atallah and Wenliang Du. **Secure Multi-Party Computational Geometry**. In *Lecture Notes in Computer Science, 2125, Springer Verlag. Proceedings of 7th International Workshop on Algorithms and Data Structures (WADS 2001)*, Providence, Rhode Island, USA. Pages 165-179. August, 8-10, 2001.
100. Wenliang Du and Mikhail J. Atallah. **Privacy-Preserving Cooperative Scientific Computations**. In *14th IEEE Computer Security Foundations Workshop*, Nova Scotia, Canada. Pages 273-282. June 11-13 2001. (Acceptance Ratio: 21/54).
101. Wenliang Du and Mikhail J. Atallah. **Protocols for Secure Remote Database Access with Approximate Matching**. In *the First Workshop on Security and Privacy in E-Commerce, in association with the 7th ACM Conference on Computer and Communications Security*, Athens, Greece. Nov. 1-4 2000.
102. Wenliang Du and Aditya P. Mathur. **Testing for Software Vulnerability Using Environment Perturbation**. In *Proceeding of the International Conference on Dependable Systems and Networks (DSN 2000), Workshop On Dependability Versus Malicious Faults*, New York City, NY, USA. Pages 603-612. June 25-28 2000.
103. Wenliang Du, Praerit Garg and Aditya P. Mathur. **Security Relevancy Analysis On the Registry Of Windows NT 4.0**. In *Proceeding of the 15th Annual Computer Security Applications Conference (ACSAC'99)*, Phoenix, Arizona, USA. Pages 331-340. December 6-10, 1999.
104. Wenliang Du and Aditya P. Mathur. **Categorization of Software Errors that led to Security Breaches**, In *Proceeding of the 21st National Information Systems Security Conference (NISSC'98)*, Crystal City, VA, 1998.
105. Yi Deng, Wenliang Du, Paul C. Attie, and Michael Evangelist. **A Formalism for Architectural Modeling of Concurrent Real-Time Systems**, In *Proceeding of the 8th International Conference on Software Engineering and Knowledge Engineering (SEKE'96).*

Book Chapter

106. Wenliang Du, Lei Fang, Peng Ning. **Beaconless Location Discovery in Wireless Sensor Networks**. In *Cliff Wang, Radha Poovendran, Sumit Roy (Eds), Secure Localization and Time Synchronization for Wireless Sensor and Ad Hoc Networks*, Springer, 2007.
107. Peng Ning, Donggang Liu, Wenliang Du. **Secure and Resilient Location Discovery in Wireless Sensor Networks**. In *Cliff Wang, Radha Poovendran, Sumit Roy (Eds), Secure Localization and Time Synchronization for Wireless Sensor and Ad Hoc Networks*, Springer, 2007.
108. Wenliang Du and Mikhail J. Atallah. **Protocols for Secure Remote Database Access with Approximate Matching**. In *Recent Advances in Secure and Private E-Commerce*, Kluwer Academic Publishers, 2001

Invited Research Talks

1. **Internet Emulator**. Invited to give talks at 25 universities and institutes around the world from September 2022 to August 2023.
2. **Smartphone Security**. Invited to give talks at Korea Internet & Security Agency (6/22/2016), KAIST: Korea Advanced Institute of Science and Technology (6/21/2016), Korea National Security Research Institute (6/21/2016), Jinan University (10/29/2015), Palo Alto Networks (10/6/2015), Samsung Research America (10/5/2015), Forum on Frontiers of Science and Technology: Software and Network Security (11/13/2014), Indiana University-Purdue University Indianapolis (10/10/2014), University of Michigan-Dearborn (10/3/2014), Temple University (9/26/2014), Virginia Tech (9/5/2014), Rochester Institute of Technologies (3/24/2014), SUNY Fredonia (3/19/2014), University of South Florida (2/19/2014), University at Buffalo (9/26/2013), Air Force Research Lab (8/13/2013), Syracuse Research Corporation (7/16/2013), Institute of Software in China (5/17/2013), Peking University (5/16/2013), Microsoft Research Beijing (5/15/2013), McMaster University (4/24/2013), Penn State Erie (4/23/2013), Department Colloquium at the University of Florida (2/18/2013), Dowling College (2/4/2013), IEEE Syracuse Section Computer Society Chapter (1/30/2013), Itheca College (11/14/2012), and the 25th School of Computing & Information Sciences Anniversary at the Florida Internation University (11/9/2012).
3. **Web Security**. Invited talks at Microsoft Research (Redmond, WA, 7/28/2011), Computer Science Colloquia talk at University of Massachusetts Lowell (12/1/2010), and the 25th Annual WG 11.3 Conference on Data and Applications Security and Privacy (Richmond, VA, 7/11/2011), the University of Science and Technology of China (5/11/2010), and Beijing Institute of Technology (5/10/2010).
4. **The SEED project: Security Education**. Invited talks at University of Science and Technology of China (5/12/2010). Invited panelists at the NICE (National Initiative for Cybersecurity Education) Track 2 Coalition organizational meeting (11/5/2010), and the Annual Conference on Education in Information Security (9/18/2006).
5. **Securing Wirless Sensor Networks**. Invited talks at Air Force Research Lab at Rome (11/15/2007), The IEEE Joint Chapter for Communications and Aerospace at Rochester (6/6/2006), Computer Science Graduate Seminar at Wayne State University (12/13/2005), Clarkson University (4/16/2004), CERIAS Security Seminar, Purdue University (3/31/2004),
6. **Privacy-Preserving Data Mining**. University of Pittsburgh (4/18/2006), Stevens Institute of Technology (4/18/2005), DIMACS workshop on privacy-preserving data mining (3/17/2004), University of Maryland College Park (10/27/2003).
7. **Tutorial: Using Instructional Operating System to Teach Computer Security Courses**. A tutorial at the 11th ACM Conference On Computer And Communication Security (CCS). Alexandria, VA, November 10, 2005.
8. **Security for Grid-based computing systems – The challenges**, an invited panelist at SACMAT, June 2004.

Activities

- December 2019: Held a 5-day SEED workshop in Riyadh, Saudi Arabia.
- 2015 - 2019: Organized two 4-day SEED workshops each year to train university and college professors from all over the US to use the SEED labs that we developed.
- Editorial Board Member of the International Journal of Security and Networks ('08-'10).
- Guest Editor of *Journal of Computer Security, Special Issue on Security of Ad Hoc and Sensor Networks*, 2006.
- Tutorials Chair of the 13th & 14th ACM Conference on Computer and Communications Security (CCS), 2006 and 2007.
- Program Chair
  - The 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN'05).
  - The 2nd Workshop on Privacy Preserving Data Mining (PPDM'03). In conjunction with IEEE ICDM'03.
- Program Committee
  - CCS ('07 - '09, '13 - '14): The ACM Conference on Computer and Communication Security.
  - ESORICS ('09 - '14),: European Symposium on Research in Computer Security.
  - NDSS('13): The Network and Distributed System Security Symposium.
  - ASIACCS ('13 - '19): ACM Symposium on InformAtion, Computer and Communications Security.
  - ICDCS ('08 - '12): The International Conference on Distributed Computing Systems.
  - WWW ('11): The International World Wide Web Conference.
  - ICDE'10: The 26th IEEE International Conference on Data Engineering.
  - WiSec ('08 - '09, '16): The ACM Conference on Wireless Network Security.
  - ISDPE'07: International Symposium on Data, Privacy, and E-Commerce.
  - ICICS'06: International Conference on Information and Communications Security.
  - PADM'06: International Workshop on Privacy Aspects in Data Mining.
  - SDM ('04 and '05): SIAM International Conference on Data Mining.
  - SASN ('04 - '06): ACM Workshop on Security of Ad Hoc and Sensor Networks.
  - WiSe ('05 and '06): ACM Workshop on Wireless Security.
  - ICPADS'05: The 11th International Conference on Parallel and Distributed Systems.
  - NSPW'02: ACM New Security Paradigm Workshop.
- Journal Reviewer
  - ACM Transactions on Information and System Security (TISSEC)
  - IEEE Transactions on Dependable and Secure Computing (TDSC),
  - IEEE Transactions on Sensor Networks (TOSN),
  - IEEE Transactions on Parallel and Distributed Systems (TPDS),
  - IEEE Transactions on Knowledge and Data Engineering (TKDE),
  - IEEE Transactions on Mobile Computing (TMC),
  - IEEE/ACM Transactions on Networking (ToN),
  - IEEE Transactions on Computers,
  - IEEE Security and Privacy Magazine,
  - IEEE Internet Computing,
  - IEEE Communications Letters,

  - Journal of Computer Security,
  - Ad Hoc Networks journal,
  - Wireless Networks,
  - Journal of Database Management,
  - Journal of Intelligent Information Systems,
  - Data Mining and Knowledge Discovery.
- Member of ACM and IEEE.

Teaching

CSE644: Internet Security (2004 - 2020)
CSE643: Computer Security (2002 - 2021)
CSE484: Introduction to Computer & Network Security (2004 - 2021)
CSE691: Android Programming (2013 - 2017)
CIS700: Smartphone Security (2012 - 2014)
CIS700: Web Security (2010)
CIS700: Advanced Cryptography (2009)
CIS700: Wireless Networks Security (2003 - 2007)
CIS351: Data Structures (2003)
CSE555: Principles of Programming I (2001 -2003)