

Wenliang (Kevin) Du's Curriculum Vitae

Current Address: 4-206 Science & Technology Building, Syracuse, NY 13244, USA
+1 315 443-9180, wedu@ecs.syr.edu, <http://www.cis.syr.edu/~wedu/>

Research Areas Computer and Information Security, Web Security & Privacy, Privacy Preserving Data Mining, and Computer Security 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: Mikhail J. Atallah and 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: Yi Deng

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

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

Syracuse University, Syracuse, NY *Assistant Professor*
Department of EECS **Aug. 2001 – June 2007**

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

Honors and Awards

- Best Paper Award in the 5th Annual Symposium on Information Assurance (ASIA 2010).
- Best Paper Award in the 11th Pacific-Asia Conference on Knowledge Discovery and Data Mining (PAKDD 2007).
- Best Paper Award in the 19th IEEE International Parallel & Distributed Processing Symposium (IPDPS 2005).
- Presidential Fellowship (1994-1996), Florida International University.
- Guo Mo-ruo Award (1992), University of Science & Technology of China.
- First-class prize winner in the National High-school Mathematics Contests (1987 & 1988).

- Member of Upsilon Pi Epsilon Honor Society.

Fundings

1. To Configure or to Implement, that is the Access Control Question for Web Applications. NSF Trustworthy Computing, 09/2010-08/2013, \$471,970, PI.
2. SEED: Developing Instructional Laboratories for Computer Security Education. NSF-CCLI (Phase II), 01/2007-12/2010, \$451,682, PI.
3. Designing Laboratory Materials for Computer System Security Courses Using Minix Instructional Operating System. NSF-CCLI (Phase I), 01/03-12/05, \$74,984, PI.
4. Data Fusion and Visualization. JP Morgan Chase, 05/2010 - 11/2011, \$500,000, co-PI.
5. Identity Management. JP Morgan Chase, 01/2008 - 01/2009, \$200,000, co-PI.
6. Efficient and Resilient Key Management for Wireless Sensor Networks. ARO, 5/05-4/08, \$360,000, PI.
7. Collaborative Research: Trustworthy and Resilient Location Discovery in Wireless Sensor Networks. NSF CyberTrust, 9/04-8/07, \$150,000, PI.
8. Collaborative Research: ITR: Distributed Data Mining to Protect Information Privacy. NSF-ITR, 8/03-7/06, \$140,418, PI.
9. Private Prediction using Selective Models. NSF-ITR, 9/02-8/05, \$220,000, PI.
10. VINE: Using Virtual Network Environment for Computer and Network Security Courses. University Vision Fund, 1/03-12/03, \$5,000, PI.

Publications

Journal

1. 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.
2. 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.
3. Zhouxuan Teng and Wenliang Du. **A Hybrid Multi-Group Privacy Preserving Approach for Building Decision Trees.** In *Knowledge and Information Systems (KAIS)*, Springer London, August 2008.
4. Wenliang Du, Jing Deng, Yunghsiang S. Han, and Pramod Varshney. **A Key Pre-distribution 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.
5. 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.
6. 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.

7. 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.
8. 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.
9. 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.
10. 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)*, Vol. 11, No. 4, pages 1-39, July 2008.
11. 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.
12. Donggang Liu, Peng Ning, and Wenliang Du. **Group-Based Key Pre-Distribution in Wireless Sensor Networks.** To appear in *ACM Transactions on Sensor Networks (TOSN)*, 2008.
13. Huseyin Polat, Wenliang Du, Sahin Renckes, and Yusuf Oysal. **Private predictions on hidden Markov models.** In the *Artificial Intelligence Review*. May 2010.
14. Huseyin Polat and Wenliang Du. **Privacy-Preserving Top-N Recommendation on Distributed Data.** To appear in the *Journal of the American Society for Information Science and Technology*, 2008.
15. 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.
16. 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.

Refereed Conference & Workshop Proceedings

17. Karthick Jayaraman, Wenliang Du, Balamurugan Rajagopalan, and Steve J. Chapin. **Escudo: A Fine-grained Protection Model for Web Browsers.** In *ICDCS: The 30th International Conference on Distributed Computing Systems*, Genoa, Italy, June 21-25, 2010.
18. Wenliang Du. **SEED: 25 Hands-on Labs for Information Assurance Education.** A short topic presentation at The *Colloquium for Information Systems Security Education (CISSE)*. June 7-9, 2010. Baltimore, Maryland.
19. 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.**
20. Zutao Zhu and Wenliang Du. **Understanding Privacy Risk of Publishing Decision Trees.** In *24th Annual IFIP WG 11.3 Working Conference on Data and Applications Security (DBSec 2010)*. Rome, Italy. June 21-23, 2010.
21. Guan Wang, Tongbo Luo, Michael Goodrich, Wenliang Du, and Zutao Zhu. **Bureaucratic Protocols for Secure Two-Party Sorting, Selection, and Permuting.** In the *ACM Symposium on Information, Computer and Communications Security*. Beijing, China, April 13-16, 2010.

22. Zutao Zhu and Wenliang Du. **K-anonymous Association Rule Hiding** (short paper). In *the ACM Symposium on Information, Computer and Communications Security*. Beijing, China, April 13-16, 2010.
23. 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 *Algorithms and Data Structures Symposium (WADS)*, 21-23 August, 2009. Banff Conference Centre, Banff, Alberta, Canada.
24. Zutao Zhu, Guan Wang, and Wenliang Du. **Deriving Private Information from Association Rule Mining Results**. In *the 25th IEEE International Conference on Data Engineering (ICDE)*, Shanghai, China, March 29 - April 4, 2009. (Acceptance ratio: 16.8% = 93/554).
25. Guan Wang, Zutao Zhu, Wenliang Du, and Zhouxuan Teng. **Inference Analysis in Privacy-Preserving Data Re-publishing**. In *the 8th IEEE International Conference on Data Mining (ICDM)*, Pisa, Italy, Dec. 15-19, 2008 (short paper). (Acceptance ratio: 20% = 144/724).
26. 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).
27. 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%).
28. Sangwon Hyun, Peng Ning, An Liu, Wenliang Du, **Seluge: Secure and DoS-Resistant Code Dissemination in Wireless Sensor Networks**. To appear 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).
29. 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).
30. 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.
31. 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.
32. 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).
33. 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).
34. 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)

35. 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).
36. 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).
37. 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)
38. 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).
39. 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).
40. 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.
41. 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).
42. 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.
43. 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).
44. 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).
45. 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.
46. 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.
47. 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).
48. 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).

49. 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)
50. 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).
51. 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).
52. 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 ration 14.3% = 23/161).
53. 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).
54. 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).
55. 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).
56. 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).
57. 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).
58. Mikhail J. Atallah, Florian Kerschbaum, and Wenliang Du. **Secure and Private Sequence Comparisons.** 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)
59. 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.
60. 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.
61. 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).
62. 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.

63. 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.
64. 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.
65. 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).
66. 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.
67. 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.
68. 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.
69. 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.
70. 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

71. 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.
72. 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.
73. 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 Talks

1. **Learning by Doing: How to Make This Happen in Computer Security Education?** Invited talk at the University of Science and Technology of China, May 12, 2010.
2. **So Many Attacks on the Web: Whom should we blame?** Invited talk at the University of Science and Technology of China, May 11, 2010.
3. **So Many Attacks on the Web: Whom should we blame?** Invited talk at the Beijing Institute of Technology, May 10, 2010.

4. **Securing Wireless Sensor Networks.** Invited talk at the Air Force Research Lab at Rome, November 15, 2007.
5. **Open Source/Closed Source Software in Security Education,** invited panelist at the Annual Conference on Education in Information Security, September 18, 2006.
6. **Securing Wireless Sensor Networks.** Invited talk at the IEEE Joint Chapter for Communications and Aerospace at Rochester, June 6, 2006.
7. **Privacy-Preserving Data Mining.** University of Pittsburgh. April 18, 2006.
8. **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.
9. **Securing Wireless Sensor Networks.** Computer Science Graduate Seminar, Wayne State University. December 13, 2005.
10. **Privacy-Preserving Data Mining.** Computer Science Seminar, Stevens Institute of Technology. April 18, 2005.
11. **Security for Grid-based computing systems – The challenges,** an invited panelist at SACMAT, June 2004.
12. **Securing Wireless Sensor Networks,** Clarkson University. April 16, 2004.
13. **Securing Wireless Sensor Networks,** CERIAS Security Seminar, Purdue University. March 31, 2004.
14. **Privacy-Preserving Data Mining,** DIMACS workshop on privacy-preserving data mining. March 17, 2004.
15. **Privacy Preserving Data Mining,** Department of Computer Science, University of Maryland College Park. October 27, 2003.

Activities

- Editorial Board Member of the International Journal of Security and Networks (2008 - 2010).
- Guest Editor of *Journal of Computer Security, Special Issue on Security of Ad Hoc and Sensor Networks.*
- 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
 - WWW (2011): International World Wide Web Conference (Abuse, Security & Security track).
 - ICDCS ('08 - '11): The International Conference on Distributed Computing Systems.
 - CCS ('07 and '09): The ACM Conference on Computer and Communication Security.
 - ICDE 2010: The 26th IEEE International Conference on Data Engineering (Privacy & Security track)
 - WiSec ('08 - '09): 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.

- ASIACCS'06: ACM Symposium on InformAtion, Computer and Communications Security.
- SDM ('04 and '05): SIAM International Conference on Data Mining.
- SASN ('04, '05 and '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.
- 2002 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 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

CIS483: Introduction to Computer & Network Security (2004 - 2010)
 CIS/CSE758: Internet Security (2004 - 2010)
 CIS/CSE785: Computer Security (2002 - 2010)
 CIS700/CSE791: Web Security (2010)
 CIS700/CSE791: Wireless Networks Security (2003 - 2007)
 CIS351: Data Structures (2003)
 CSE555: Principles of Programming I (2001 -2003)
 CSE691: Computer Security Seminar (2001)