

DANFENG (DAPHNE) YAO

CURRICULUM VITAE

Department of Computer Science
Rutgers, the State University of New Jersey
Piscataway, NJ 08854-8019

732-445-2001 ext. 1188
danfeng@cs.rutgers.edu
Homepage: <http://www.cs.rutgers.edu/~danfeng/>

RESEARCH INTERESTS

User-centric security and privacy, social- and human-behavior pattern recognition, insider threats, secure information sharing, data privacy, and applied cryptography

EDUCATION

Ph.D., Computer Science, Brown University , Providence, RI	2007
M.S., Computer Science, Indiana University , Bloomington, IN	2002
B.S., Peking University , Beijing, China	1998

EMPLOYMENT

Department of Computer Science, Rutgers University, New Brunswick, NJ Assistant Professor	Jan. 2008 – Present
Department of Computer Science, Brown University Research assistant (With Professor Roberto Tamassia, Department Chair)	Aug. 2002 – Dec. 2007
CERIAS, Purdue University, West Lafayette IN Visiting scholar (With Professor Elisa Bertino and Mikhail J. Atallah)	Sep. 2006 – Dec. 2007
HP Systems Security Lab, Princeton, NJ Research intern (With Dr. Stuart Haber)	May 2006 – Aug. 2006
IAM Technology Inc., Providence, RI Consultant (With David Croston, CEO)	Apr. 2005 – May. 2007
Center of Genomics and Bioinformatics, Indiana University, Bloomington Research assistant (With Dr. Donald Gilbert)	May 2001 - Aug. 2002

TEACHING

Computer Science Department	Rutgers University
CS673 Recent Advances in Computer Security	Fall 2009
CS672 Information Security	Fall 2008
CS352 Internet Technology	Spring 2008, Spring 2009
CS500:04 Light Seminar: Secure Information Sharing	Spring 2008

HONORS

Best Poster Prize, Wireless & Optical Communications Conference	May 2009
Nomination for Microsoft New Faculty Fellowship (one per university)	Nov. 2008
Best Student Paper Award, ICICS 2006	Dec. 2006
Award for Technological Innovation from Brown University	Apr. 2006
University Fellowship, Brown University	Sep. 2002
Graduate with the Highest Honors, Peking University	Jul. 1998
IEC Fellowship, Peking University	Sep. 1996
Outstanding Student Fellowship, Peking University	Sep. 1995
SONY Fellowship, Peking University	Sep. 1995

GRANTS

1. CT - ISG: ROME: Robust Measurement in Sensor Networks. National Science Foundation (NSF). PI: Yanyong Zhang, Co-PI: Danfeng Yao and Hui Xiong. \$400,000. Sep. 2008 - Aug. 2011.
2. Secure and Flexible Information Sharing for Crisis Communication in Pervasive Computing Environments. Rutgers University Pervasive Computing Seed Grant. PI: Danfeng Yao. Co-PI: James Garnett. \$50,000. Mar. 2008 - Jun. 2009.
3. Center of Excellence for Command, Control and Interoperability. Department of Homeland Security (DHS). PI: Fred Roberts. Danfeng Yao is among the Rutgers researchers. \$15 million. 2009 - 2015.
4. The Rutgers University Research Initiative on Cybersecurity Economics (RICE). Rutgers University Academic Excellence Fund. PI: Rebecca Wright. Co-PIs: Vijay Atluri, Richard McLean, and Danfeng Yao. \$60,000. Jun. 2009 - May 2010.

PEER-REVIEWED CONFERENCES/WORKSHOPS

1. Huijun Xiong, Prateek Malhotra, Deian Stefan, Chehai Wu, and Danfeng Yao. User-Assisted Host-Based Detection of Outbound Malware Traffic. In *Proceedings of International Conference on Information and Communications Security (ICICS '09)*. Beijing, P.R. China. Dec. 2009.
2. Nitya H. Vyas, Anna Squicciarini, Chih-Cheng Chang, and Danfeng Yao. Towards Automatic Privacy Management in Web 2.0 with Semantic Analysis on Annotations. In *Proceedings of International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom)*. Washington DC. Nov. 2009.
3. Anitra Babic, Huijun Xiong, Danfeng Yao, and Liviu Iftode. Building Robust Authentication Systems With Activity-Based Personal Questions. In *Proceedings of ACM Workshop on Assurable & Usable Security Configuration (SafeConfig)*. Collocated with the ACM Conference on Computer and Communications Security. Chicago, IL. Nov. 2009.
4. Saman Zarandioon, Danfeng Yao, and Vinod Ganapathy. Privacy-aware Identity Management for Client-side Mashup Applications. In *Proceedings of the Fifth ACM Workshop on Digital Identity Management (DIM)*. Collocated with the ACM Conference on Computer and Communications Security. Chicago, IL. Nov. 2009.
5. Brian Thompson, Danfeng Yao, Stuart Haber, William G. Horne, and Tomas Sander. Privacy-Preserving Computation and Verification of Aggregate Queries on Outsourced Databases. In *Proceedings of the 9th Privacy Enhancing Technologies Symposium (PETS)*. Seattle, WA. Aug. 2009.
6. Tzvika Chumash and Danfeng Yao. Detection and Prevention of Insider Threats in Database Driven Web Services In *Proceedings of The Third IFIP WG 11.11 International Conference on Trust Management (IFIPTM)*. Pages 117-132. Jun. 2009. West Lafayette, IN.
7. Brian Thompson and Danfeng Yao. Union-Split Clustering Algorithm and Social Network Anonymization. In *Proceedings of ACM Symposium on Information, Computer & Communication Security (ASIACCS)*. Mar. 2009. Sydney, Australia.
8. Tuan Phan and Danfeng Yao. *SelectAudit*: A Secure and Efficient Audit Framework for Networked Virtual Environments. In *Proceedings of the International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom)*, **Invited paper**. Nov., 2008. Orlando, FL.
9. Saman Zarandioon, Danfeng Yao, and Vinod Ganapathy. Design and Implementation of an Open Framework for Secure Communication in Mashup Applications. In *Proceedings of Annual Computer Security Applications Conference (ACSAC)*. Dec. 8-12, 2008, Anaheim, CA.
10. Vivek Pathak, Danfeng Yao, and Liviu Iftode. Securing Location Aware Services Over VANET Using Geographical Secure Path Routing. In *Proceedings of International Conference on Vehicular Electronics and Safety (ICVES)*. September 22-24, 2008. Columbus, Ohio.

11. Vivek Pathak, Danfeng Yao, and Liviu Iftode. Improving Email Trustworthiness through Social-Group Key Authentication. *Proceedings of the Fifth Conference on Email and Anti-Spam (CEAS)*. Microsoft Research Silicon Valley, Mountain View, California. Aug 21-22, 2008.
12. Danfeng Yao. An Ad Hoc Trust Inference Model for Flexible and Controlled Information Sharing. In *Proceedings of International Conference on Security and Management (SAM)*. 555-561. Las Vegas, NV. July, 2008.
13. Stuart Haber, Yasuo Hatano, Yoshinori Honda, William Horne, Kunihiko Miyazaki, Tomas Sander, Satoru Tezuka, and Danfeng Yao. Efficient signature schemes supporting redaction, pseudonymization, and data deidentification. In *Proceedings of ACM Symposium on Information, Computer & Communication Security (ASIACCS)*. 353-362. Mar. 2008.
14. Danfeng Yao, Roberto Tamassia, and Seth Proctor. Private Distributed Scalar Product Protocol With Application To Privacy-Preserving Computation of Trust. In *Proceedings of IFIPTM 2007 – Joint iTrust and PST Conferences on Privacy, Trust Management and Security*. Moncton, New Brunswick, Canada. Jul. 2007.
15. Isabel F. Cruz, Roberto Tamassia, and Danfeng Yao. Privacy-Preserving Schema Matching Using Mutual Information. In *Proceedings of the 21th Annual IFIP WG 11.3 Working Conference on Data and Applications Security (DBSec '07)*. 93-94. Redondo Beach, CA. Jul. 2007.
16. Danfeng Yao, Yunhua Koglin, Elisa Bertino, and Roberto Tamassia. Decentralized Authorization and Data Security in Web Content Delivery. In *Proceedings of the 22nd ACM Symposium on Applied Computing (SAC '07)*, Special Track on Web Technologies. 1654-1661. ACM Press. Seoul, Korea. Mar. 2007.
17. Danfeng Yao, Keith B. Frikken, Mikhail J. Atallah, and Roberto Tamassia. Point-Based Trust: Define How Much Privacy Is Worth. In *Proceedings of the Eighth International Conference on Information and Communications Security (ICICS '06)*. LNCS 4307, pages 190-209. Springer. Raleigh, NC. Dec. 2006. **Best Student Paper Award**.
18. Danfeng Yao and Roberto Tamassia. Cascaded Authorization with Anonymous-Signer Aggregate Signatures. In *Proceedings of the Seventh Annual IEEE Systems, Man and Cybernetics Information Assurance Workshop (IAW '06)*. West Point, NY. Jun. 2006.
19. Michael T. Goodrich, Roberto Tamassia, and Danfeng Yao. Notarized Federated Identity Management for Increased Trust in Web Services. In *Proceedings of the 20th Annual IFIP WG 11.3 Working Conference on Data and Applications Security (DBSec '06)*. LNCS 4127, pages 133-147. Springer. Sophia Antipolis, France. Jul. 2006.
20. Danfeng Yao, Michael Shin, Roberto Tamassia, and William H. Winsborough. Visualization of Automated Trust Negotiation. In *Proceedings of the Workshop on Visualization for Computer Security (VizSEC '05) in Conjunction with Vis 2005 and InfoVis 2005*. Pages 65-74. IEEE Press. Minneapolis, MN. Oct. 2005.
21. Danfeng Yao, Roberto Tamassia, and Seth Proctor. On Improving the Performance of Role-Based Cascaded Delegation in Ubiquitous Computing. In *Proceedings of the IEEE/CreateNet Conference on Security and Privacy for Emerging Areas in Communication Networks (SecureComm '05)*. Pages 157-168. IEEE Press. Athens, Greece. Sep. 2005.
22. Michael T. Goodrich, Roberto Tamassia, and Danfeng Yao. Accredited DomainKeys: A Service Architecture for Improved Email Validation. In *Proceedings of the Second Conference on Email and Anti-Spam (CEAS '05)*. Stanford University, CA. Jul. 2005.
23. Danfeng Yao, Nelly Fazio, Yevgeniy Dodis, and Anna Lysyanskaya. ID-Based Encryption for Complex Hierarchies with Applications to Forward Security and Broadcast Encryption. In *Proceedings of the 11th ACM Conference on Computer and Communications Security (CCS '04)*. Pages 354-363. ACM Press. Washington, DC, Oct. 2004.

24. Roberto Tamassia, Danfeng Yao, and William H. Winsborough. Role-Based Cascaded Delegation. In *Proceedings of the ACM Symposium on Access Control Models and Technologies (SACMAT '04)*. Pages 146-155. ACM Press. Yorktown Heights, NY, Jun. 2004.

JOURNALS AND BOOK CHAPTERS

25. Roberto Tamassia, William H. Winsborough, Nitya Vyas, and Danfeng Yao. Independently-Verifiable Decentralized Role-Based Delegation. *IEEE Transactions on Systems, Man, and Cybernetics, Part A*. Jul. 2009. *To appear*.
26. Danfeng Yao, Nelly Fazio, Yevgeniy Dodis, and Anna Lysyanskaya. Forward-Secure Hierarchical IBE with Applications to Broadcast Encryption Schemes. In *Cryptology and Information Security Series on Identity-Based Cryptography*. Editors: Marc Joye and Gregory Neven. IOS Press. Oct. 2008.
27. Michael T. Goodrich, Roberto Tamassia, and Danfeng Yao. Notarized Federated Identity Management for Increased Trust in Web Services. *Journal of Computer Security*, 16(4): 399-418. 2008.
28. Danfeng Yao, Keith Frikken, Mike Atallah, Roberto Tamassia. Private Information: To Reveal or Not To Reveal. *ACM Transactions on Information and System Security (TISSEC)*. 12(1). Feb. 2008.
29. Yunhua Koglin, Danfeng Yao, and Elisa Bertino. Secure Content Distribution by Parallel Processing from Cooperative Intermediaries. *IEEE Transactions on Parallel and Distributed Systems*. 19(5): 615-626. 2008.
30. Danfeng Yao and Roberto Tamassia. Compact and Anonymous Role-Based Authorization Chain. *ACM Transactions on Information and System Security (TISSEC)*. 12(3). Mar. 2009.

PAPERS IN SUBMISSION

1. Jerry Rick Ramstetter and Danfeng Yao. The Applications and Security of Next-Generation User-Centric Wireless Systems *Future Internet, Special Issue on Security for Next Generation Wireless and Decentralized Systems*. Invited submission. Jan. 2010.
2. Deian Stefan, Chehai Wu, Danfeng Yao, and Gang Xu. Provenance Verification Approach in Host-Based Malware Detection With Trusted User Inputs. *Network and Distributed System Security '10*). Submitted.
3. Chih-Cheng Chang, Brian Thompson, Hui Wang, and Danfeng Yao. Anonymous Reviews: Privacy Preserving Publishing of Recommendation Data. *ACM Symposium on Information, Computer & Communication Security (ASIACCS '10)*. Submitted.
4. Qian Yang, Danfeng Yao, James Garnett, and Kaitlyn Muller. A Trust Inference Model for Flexible and Controlled Information Sharing During Crises. *Journal of Contingencies and Crisis Management*. Submitted.

PRESENTATIONS

1. Host-Based and User-Centric Detection of Drive-By-Download Attacks. DIMACS Fall Mixer. Rutgers University. Sep. 2009.
2. Cryptographic Provenance Verification Approach in Malware Detection With Trusted User Inputs. *Security and Privacy Day*. Rutgers University. May 2009.
3. Personalized Security With Trusted User Inputs For Botnet Detection. *Virginia Tech Computer Science Departmental Seminar*, Blacksburg, VA. May 2009.

4. Keystroke Dynamic Authentication With Trusted User Inputs For Human-Behavior Driven Bot Detection. *Purdue University Computer Science Departmental Seminar*, West Lafayette, IN. Mar. 2009.
5. Keystroke Dynamics Authentication and Human-Behavior Driven Bot Detection. *Departmental Seminar*. Stevens Institute of Technology, Department of Electrical and Computer Engineering. Hoboken, NJ. Oct. 2008.
6. Compact and Anonymous Role-Based Authorization Chains. *NIST Workshop on Applications of Pairing Based Cryptography: Identity Based Encryption and Beyond*. NIST at Gaithersburg, MD. Jun. 2008.
7. Efficient signature schemes supporting redaction, pseudonymization, and data deidentification. *BSF/DIMACS/DyDAn Workshop on Data Privacy*. Rutgers University, NJ. Jan. 2008.
8. Private Information: To Reveal Or Not To Reveal. *Departmental Seminars*. Department of Computer Science at Rutgers University, Texas A&M University, Washington University at St. Louis, and Indiana University - Purdue University at Indianapolis; Department of Electrical and Computer Engineering at Iowa State University and Purdue University. Spring 2007.
9. Trust and Service Negotiations Using WSPL. Sun Microsystems Lab, Burlington MA. Nov. 2003.

POSTERS

1. Ensuring Host Integrity With Cryptographic Provenance Verification. Deian Stefan, Chehai Wu, Danfeng Yao, and Gang Xu. ACM Computer and Communications Security (CCS). Chicago, IL. Nov. 2009.
2. Huijun Xiong, Chih-Cheng Chang, Prateek Malhotra, and Danfeng Yao. Exploring the Human-Behavior Driven Detection Approach in Identifying Outbound Malware Traffic. USENIX Security Symposium. Montreal, Canada. Aug. 2009.
3. Brian Thompson, Chih-Cheng Chang, Hui Wang, and Danfeng Yao. Privacy-Aware Publishing of Netflix Data. IEEE Symposium on Security and Privacy. Oakland, CA. May 2009.
4. Chehai Wu and Danfeng Yao. CompareView - A Provenance Verification Framework for Detecting Rootkit-Based Malware. IEEE Symposium on Security and Privacy. Oakland, CA. May 2009.
5. Jiawei Sun, Bernhard Firner, Danfeng Yao, and Yanyong Zhang. Efficient and Fault-Tolerant Detection of Attacks in RFID Asset Tracking Systems. Wireless and Optical Communications Conference (WOCC). Newark, NJ. May 2009.
6. Deian Stefan, Danfeng Yao, and Gang Xu. Trusted-input for anomaly detection of botnets. The Third Annual DHS University Network Summit. Washington, D.C. Mar. 2009.
7. Qian Yang and Danfeng Yao. EmAuth: a Framework for Cross-Organizational Vouching. *The Eighth New Jersey Universities Homeland Security Research Consortium Symposium*. Princeton University, NJ. Dec. 2008.
8. Huijun Xiong and Danfeng Yao. Human-Behavior Driven Personalized Anomaly Detection. *Security and Privacy Day*. IBM Research, NY. Dec. 2008.
9. Brian Thompson and Danfeng Yao. Social Role-Preserving Graph Anonymization Using Clustering. *Security and Privacy Day*. IBM Research, NY. Dec. 2008.
10. Nitya H. Vyas and Danfeng Yao. Folksonomy Meets Text Inference: Automatic Privacy Management For Web 2.0. *Security and Privacy Day*. IBM Research, NY. Dec. 2008.

- Tuan Phan and Danfeng Yao. Secure and Efficient Audit Framework for Multi-Player Online Games. *Security and Privacy Day*. SUNY, Stony Brook. May 2008.

STUDENTS

Vivek Pathak (Ph.D. graduated, on faculty at Stevens Institute of Technology Computer Science Department, co-advised with Prof. Liviu Iftode)
 Chehai Wu (M.S. graduated, Oct., 2009, first job at AppFolio.com)
 Brian Thompson (4th-year Ph.D. student)
 Chih-Cheng Chang (3rd-year Ph.D. student)
 Huijun Xiong (2nd-year Ph.D. student)
 Qiang Ma (2nd-year Ph.D. student)
 Saman Zarandioon (4th-year Ph.D. student)
 Nitya H. Vyas (2nd-year M.S. student, Co-op at Siemens Research in 2009)
 Deian Stefan (Undergraduate at The Cooper Union, NYC, REU '08)
 Alexander Crowell (Undergraduate at Rutgers University, REU '09)
 Prateek Malhotra (Undergraduate at Rutgers University, Class '12)
 Anitra Babic (Undergraduate at Chestnut Hill College, REU '09)
 Andre Madeira (Ph.D. thesis committee '09)
 Wenxuan Zhang (Ph.D. graduated, thesis committee member) currently at Atypon Systems.
 Gouri Dongaonkar (Undergraduate, Rutgers Department of Electrical and Computer Engineering)

STUDENT AWARDS AND HONORS

Saman Zarandioon, Huijun Xiong, ACM CCS Student Travel Grant,	Oct. 2009
Chih-Cheng Chang, USENIX Security Symposium Student Travel Award,	Aug. 2009
Brian Thompson, Chehai Wu, IEEE Symposium on Security and Privacy Travel Awards,	May 2009
Brian Thompson, DHS DyDAn Fellowship,	Jan. 2009 - Aug. 2011
Deian Stefan, Botnet Biometrics Work Featured in NSF Highlights,	Jan. 2009
Saman Zarandioon, ACSAC Student Conferenceship,	Dec. 2008
Vivek Pathak, Rutgers University Graduate School Travel Award,	Nov. 2008

SERVICES

Publicity and Awards Committee, Rutgers Computer Science	2008-2009
Admission Committee, Rutgers Computer Science	2008-2009

PROFESSIONAL ACTIVITIES

- Reviewer for *ACM Transactions on Information and System Security (TISSEC)*, *Journal of Computer Security*, *IEEE Transactions on Dependable and Secure Computing*, *Knowledge and Information Systems*, *IEEE Transactions on Knowledge and Data Engineering*, *IEEE Journal on Selected Areas in Communications*, *Frontiers of Computer Science in China*, *Journal of Systems and Software*, *IEEE Internet Computing*, *Usenix Technical '08*, *IEEE Symposium on S & P '07*, *ICDE '07*.
 Program Committee member for *IEEE GLOBECOM '10*, *IFIPTM '10*, '09, *WWW '10*, '09, *IEEE ICCCN '09*, *Create-Net/ICST CollaborateCom '09*, '08, *ACM SAC '07*, *IEEE PADM '07*.
- NSF panelist '08.
- Long-term research collaborations with HP Lab, Sun Microsystems, and IAM Technology. Co-organizer for Northeast Security and Privacy Day at Rutgers University, May 2009.
- Active member in Center for Discrete Mathematics & Theoretical Computer Science (DIMACS), DHS Center of Excellence in Command, Control and Interoperability (CCI). Rutgers Center of Information Assurance (RCIA).

COLLABORATORS

Rebecca Wright, Liviu Iftode, Vinod Ganapathy, Dimitris Metaxas, S. Muthu Muthukrishnan, Michael Littman, Rutgers CS;

Yanyong Zhang, Rutgers ECE; *Vijay Atluri, Hui Xiong*, Rutgers MSIS; *Jimmy de la Torre*, Rutgers Graduate School of Education; *Mor Naaman*, Rutgers SCILS;

James Garnett, Rutgers Public Policy & Admin.; *Nina Fefferman* Rutgers Ecology, Evolution, & Natural Resources;

Fred Roberts, Tamra Carpenter, Midge Cozzens, James Abello, Rutgers DIMACS;

Elisa Bertino, Mikhail Atallah, Purdue CS;

Francis Quek, Naren Ramakrishnan, Virginia Tech CS;

Anna Lysyanskaya, Brown CS; *Yevgeniy Dodis* NYU CS;

Tina Eliassi-Rad, Lawrence Livermore National Lab

Stuart Haber, Tomas Sander, William Horne, Prasad Rao, HP Lab; *Seth Proctor*, Sun Microsystems;

David Croston, IAM Tech.

PATENT

1. Deian Stefan, Chehai Wu, and Danfeng Yao. Robust Keystroke Authentication and Input-Traffic Correlation Analysis For Accurate Bot Detection. Provisional Patent Filed. Rutgers University. Mar., 2009.
2. Stuart Haber, William Horne, Tomas Sander, and Danfeng Yao. Integrity Verification of Pseudonymized Documents. HP Labs. Sep. 2007. U. S. Patent Filed. Application number: 11/854413.

PERSONAL INFORMATION

Female, permanent resident of United States.