SALVATORE JOSEPH STOLFO

Curriculum Vitae

As of April 7, 2015
(URL:http://www.cs.columbia.edu/~sal/)

Education

Ph.D. Computer Science, October 1979. Courant Institute of Mathematical Sciences, New York University.

Dissertation: *Automatic Discovery of Heuristics for Nondeterministic Programs from Sample Execution Traces*, (fully supported fellowship student).

M.S. Computer Science, June 1976. Courant Institute of Mathematical Sciences, New York University.

B.S. Computer Science and Mathematics, June 1974. Brooklyn College of the City University of New York.

Research Interests

Computer Security, Data Mining-based Intrusion Detection Systems, Machine Learning, Knowledge Discovery in Databases and Data Mining, Parallel Processing and Systems.

Publication H-Index: 65 as of January 2015 (Google Scholar http://scholar.google.com/citations?user=DknsgF8AAAAJ&hl=en)

Professional Employment

- Tenured Professor of Computer Science, Columbia University, June 1997 - present.
- Tenured Associate Professor of Computer Science, Columbia University, May 1986 - June 1997.
- Acting Chairman, Computer Science Department, Columbia University, November 1986 - June 1987.
- Associate Professor of Computer Science, Columbia University, July 1984 - May 1986.
- Assistant Professor of Computer Science, Columbia University, July 1979 - June 1984.
- Lecturer, Department of Computer and Information Science, Brooklyn College of the City University of New York, 1974-1978.

Consulting and Professional Activities

Consultant and Advisor to Government

- Testimony before the DNI Cybersecurity Research Commission, Jan, 2013
- National Academies Panel on Digitization and Communications Science, 2012-2014.
- ODNI/NSA R6 Computational CyberSecurity in Compromised Environments (C3E) Workshop, 2010.
- DARPA IPTO Insider Threat Mitigation Workshop, June 2010.
- DARPA TCTO CyberBio Idea Summit Member, March 2010.
- NSA R6 Steering Committee on Analytics for Cyber Defense, a CNCI Research Workshop, 2009.
- Cyber Security Research Roadmap Invitational Workshop, Oct 7-9, 2008.
- National Academies National Research Council/Naval Studies Board Committee on Information Assurance for Network-Centric Naval Forces, 2008, 2009.
- DARPA IPTO Futures Panel, 2007, 2008.
- DARPA Strategic Information Assurance Program, 2000.
- NSF for Electrical and Computer Engineering Department of the University of Puerto Rico, 1995.
- New York State Science and Technology Foundation, New Business Evaluation, 1989.
- NSF Site Visit Team for NSF, February, 1993.
- NSF Experimental System Program Oversight Committee, July 7, 1989.
- High Tech Subcommittee of the New York City Partnership, 1987 (chaired by J. Lederberg of Rockefeller Univ.).

Member of Formal Committees

- National Academies Panel on Digitization and Communications Science, 2012-2014.
- National Academies National Research Council/Naval Studies Board Committee on Information Assurance for Network-Centric Naval Forces, 2008-2010.
- National Cyber Defense Initiative Steering Committee, 2008.
- Congressional e-Government Task Force, Internet Caucus Advisory Committee, 2000-2001.
- Visa 3D Secure Authenticated Payments Vendor Program, 2000-2001.

Director of Centers

- Center for Applied Research in Digital Government Information Systems 1998.
- Center for Advanced Technology for Computers and Information Systems, School of Engineering and Applied Science, Columbia University, October 1988 - June 1991. (Designated by New York State Science and Technology Foundation.)

Chief Science Advisor

- Allure Security Technology, Inc.
- CounterStorm (formerly System Detection Inc.), 2001-2006.
- iPrivacy, LLC, (on leave of absence from Columbia), 2000 – 2001.
- Fifth Generation Computer Corp., 1984-1988.

Editorial Board Member

- IEEE Security and Privacy Special Issue on the Science of Security, co-Editor, 2010-2014..
- IEEE Security and Privacy Special Issue on Privacy-Preserving Sharing of Sensitive Information, co-Editor, 2009-2010.
- IEEE Security and Privacy Special Issue on Insider Threat, co-Editor, 2009.
- Journal on Knowledge Discovery and Data Mining, 2005-2008.
- IEEE Security and Privacy, 2005-2008.
- IEEE Signal Processing Special Issue, 2007.
- Machine Learning Journal Special Issue on Integrating Multiple Learned Models for Machine Learning, 1998.
- Journal of Intelligent Information Systems, (Springer, Publishers), 1995-present.

Chair and Co-Chair, Workshops and Conferences

- RAID 2013, PC Chair, 2012-2013.
- RAID 2012, PC Co-Chair, 2011-2012.
- NSF National Cyber Defense Initiative Financial Industry Workshop, Oct 2009.
- ARO/FSTC/I3P Insider Threat Workshop 2007
- NSF/US Department of the Treasury, Workshop on Resilient Financial Information Systems, 2005.
- International Conference on Knowledge Discovery in Databases and Data Mining 2000.
- NSF Workshop on Research and Development (R&D) Opportunities in Federal Information Services, 1996-1997.
- AAAI-97 Workshop on Fraud Detection, 1997.
- AAAI-96 Workshop on Integrating Multiple Models for Improving and Scaling Machine Learning Systems, 1996.

Invited Speaker (recent)

- DHS S&T, Embedded System Insecurity, Mar 2013.
- RSA Conference, Breaking Research Session, Advanced Firmware Security, San Francisco, Feb 2013.
- NSF SATC Cyber Café talk, Scalable Deception, Nov 2, 2012.
- West Point Cyber Warrior Club, Automated Reverse Engineering, Nov 5, 2012
- IEEE Webinar to LockHeed Martin, Active Defense, Nov 8, 2012.
- Atlantic Counsel Workshop on Cyber Offense Strategies, Active Defense, Oct 2012.
- DHS PI Meeting, Infrastructure Protection, Oct 2012.
- Insider Threat, I3P 10Year Meeting, National Press Club, Washington, DC, Oct 2012.
- Office of the Secretary of Defense, Scalable Deception, September, 2012.

- Little 10+ IT Auditors Group Annual Meeting, Firmware Risks, June 2012.
- US Army/DARPA, Decoy Technology, Jan 2012
- Defense Science Board, Security Metrics, March 2011
- DHS ITTC Meeting, SRI, June 2011.
- FS Roundtable/BITS, R&D Security Sub-committee, Results of wide area scan, Feb 2011.
- ARO Workshop on Moving Target Defense, Oct 25, 2010
- Cyber Security and Information Intelligence Research Workshop, April 2009.
- InfoSec Research Council, Nov 2008.
- Computer Associates, Insider Threats, Oct 2008.
- Dagstuhl Workshop on Insider Threat, July 2008.
- FORTH Research Institute, Crete, Greece, July 2008.
- ACNS 2008, June 2008.
- NIPS 07 Workshop on Adversarial Learning in Computer Security, Dec 2007
- DIMACS security seminar, April 2006.
- Global Security Consortium, Nov 2005
- DHS/OSTP Invitation only workshop on Critical Infrastructure Protection, Wash. DC, June 2005..
- Security Leadership Conference, May 2005.
- ISMIS Conference, May 2005.
- High Tech Crimes Organization, May 2005.
- Infosec, Collaborative Security, Dec 2004.
- DARPA Application Communities workshop, group leader, Oct 2004.
- Federal Aviation Administration, "Behavior-based Computer Security", January, 2004.
- InfoSec Research Council Meeting, Hard Technical Problems, "Behavior-based Computer Security", December, 2003.
- Int. Workshop on Data Mining for Security Applications, IEEE ICDM-2003, November, 2003.
- Griffiss Institute Conference, "Behavior-based Computer Security", November, 2003.
- *Time* Magazine Board of Technologists, Panel discussion and interview, Oct. 8, 2003.
- International Workshop on Mathematical Methods, Models and Architectures for Computer Networks Security", St. Petersburg, Russia, September 20-24, 2003.
- Government Convention on Emerging Technologies, Defending America Together: The New Era, Las Vegas, Jan, 2003.
- NIST ACIT Workshop on Insider Threat, Feb 2003.
- Griffiss Institute Meeting on Information Assurance and Cyber Security, Utica, Feb 2003,
- Polytechnic University, May 2003.
- Workshop on Machine Learning in Computer Intrusion Detection, GMU, Sept 2003.
- Super Computing Conference 2000, Keynote.
- IBM KDD Colloquium, May, 1999.
- Advance Information Technologies for Government Conference, Washington D.C., September, 1998, Keynote.

Invited Panelist

- RSA Conference 2012, Panelist on Embedded System Security research, Feb 2012
- RSA Conference 2011, Panelist on Future Cybersecurity research, Feb 2011
- Cyber Security and Information Intelligence Research Workshop, April 2009.
- KDD98, Distributed Data Mining Workshop, August, 1998.
- EXPO ITCA '98 Collaborative Communications, Microsoft's "Lock", March 1998.
- New York Bar Association Meeting on Antitrust Law, and DOJ vrs. Microsoft, February, 1998.
- New York Academy of Science/Mitretek Systems Workshop on Issues in Internet Payment Systems, January 1998.
- AI Meets the Real World Conference, Stamford, CT, September 1998.
- NSF CAREER Program, February 1997.
- ARPA-ITO General PI Meeting, Dallas, October, 1996.
- 4th International Workshop on Research Issues in Data Engineering - Active Databases, Houston, TX, Feb. 1994.
- Tools with AI Conf., Washington, D.C., November, 1992.

- NSF Program on Scientific Databases, July 1991

Invited Participant

- NSF Workshop on Future of Trustworthy Computing, Oct 28, 2010
- ARO Workshop on Moving Target Defense, Oct 25, 2010
- ODNI/NSA R6 Computational Cybersecurity in Compromised Environments (C3E) Workshop, 2010.
- DARPA IPTO Insider Threat Mitigation Workshop, June 2010.
- DARPA TCTO CyberBio Idea Summit Member, March 2010.
- ONR/NSF/DHS Workshop on Cyber security Data Gap Analysis, MIT, Oct, 2009.
- Schloss Dagstuhl Seminar on Insider Threat, Wadern, Germany, 2008.
- DARPA ISAT study on machine learning research, 2006.
- NSA/DTO invitation only workshops on privacy research for the Intelligence Community 2006
- ARDA Advanced Malware Roadmap and Challenge Problem Workshops, 2005.
- Briefings on Columbia IDS Research at White House, Office of Secretary of Defense, DISA, Mitre, CISCO, EDS, Symantec, NSIE, Rome Labs, Lucent, InQTel, Ft. Meade, SAIC, ARDA.
- DARPA Information Assurance and Survivability Workshop, St. Louis, May, 1999.
- White House OSTP, DOE, NSC Invitation Only Workshop on Detection of Malicious Code, Intrusions, and Anomalous Activity, Washington, D.C., February, 1999.
- Schloss Dagstuhl Seminar on Active Databases, Wadern, Germany, March, 1994.
- Check Truncation Project, Financial Systems Technology Consortium.
- First DARPA Workshop on Intelligent Information Integration Systems, Knowledge Acquisition Working Group, Reston, VA, March 1993.
- NSF Workshop on HPCC and AI, February 1992.
- Citicorp Strategic Technology Evaluation Program, Citicorp, June 1988 - 1994.

Program Committee Member (recent)

- WRIT 2013 (Workshop on Insider Threat) PC
- RAID 2013 PC Chair
- ACM CCS 2012
- RAID 2012 PC Co-Chair
- *IEEE HST 2011*
- CAEIA-IT Workshop, 2010.
- ACM CCS 2007, 2008, 2013.
- CEAS 2006.
- DHS CATCH 2009.
- RAID 2005, 2006, 2007, 2008, 2012, 2013.
- Usenix Security 2006.
- DIMVA 2009.
- IEEE Security and Privacy, Oakland, 2006.
- Int. Conference on KDD, ACM, 2002, 2005
- Worms 2005
- NSF/NIJ Symposium on Intelligence and Security Informatics, 2004, 2005.
- Applied Cryptography and Network Security (ACNS 2004), June 2004
- 4th IEEE Int. Conference on Data Mining 2004
- Int. Workshop Mathematical Methods, Models and Architectures for Computer Networks Security, 2003.
- DARPA DISCEX III Conference, Apr 2003.
- International Conference on Machine Learning 1998.
- International Conference on Knowledge Discovery in Databases and Data Mining 1998.
- International Conference on Knowledge Discovery in Databases and Data Mining, 1997.
- International Symposium on Modeling, Analysis and Simulation of Computer and Telecommunication Systems (MASCOTS '97), 1996-1997.
- National AI Conference, AAAI96, 1996.
- International Conference on Knowledge Discovery in Databases and Data Mining, 1996.

- 4th International Workshop on Research Issues in Data Engineering, (in conjunction with IEEE CS International Conference on Data Engineering), Houston, Tx, Feb. 1994.
- Eight International Symposium on Methodologies for Intelligent Systems, North Carolina, June 1994.
- National Conference on Artificial Intelligence, (AAAI-92), 1992.

Technical Advisory Boards

- Financial Systems Technology Consortium, Security Standing Committee, 2006.
- Risk Insight, Inc., Menlo Park, CA, 2005
- StackSafe Inc., (formerly Revive Systems, Inc.) Vienna, VA, 2006
- Griffiss Institute, NY, 2005

Expert Witness

- Computer and Communications Industry Association Amicus Brief in support of Department of Justice vrs Microsoft Corporation, November, 1997.

Session Chair

- RAID 2012
- International Joint Conference on AI, Workshop on Parallel Production Systems, France, August, 1993.
- National Conference on Artificial Intelligence, (AAAI-92), July 1992.
- IFIP Workshop on Principles of Knowledge Based Systems, Mt. Fuji, Japan, November, 1987.
- IEEE International Conference on Parallel Processing, 1985.
- Expert Systems in Government Conference, IEEE, 1985.

Consultant

- DARPA IPTO, 2008, 2009.
- StackSafe Inc. 2006-2008.
- Citicorp Strategic Technology Evaluation Program, Citicorp, June 1988 - 1994.
- AT&T Bell Laboratories (Whippany), Knowledge-Based Expert Systems Project, 1980-1985. (Implemented a working expert system, called ACE, that has developed into an AT&T product).
- Various law firms for advise on certain legal matters
- iPrivacy LLC., System Detection Inc., BAE, CACI, and various other companies

Lecturer

- Bell Telephone Laboratories, 1981.
- Department of Computer Science, New York University, 1978-1979.

Reviewer and PC's numerous journals, technical workshops and symposia, including:

- Journal of Machine Learning Research
- IEEE Homeland Security Technology
- IEEE Transactions on Dependable Systems
- IEEE Transactions on Signal Processing
- IEEE Security and Privacy
- IEEE ICDM
- IEEE Transactions on Knowledge and Data Engineering,
- IEEE Transactions on Parallel and Distributed Systems
- IEEE Computer Magazine
- IEEE Security and Privacy Symposium
- NSF/NIJ Symposium on Intelligence and Security Informatics
- Conf on Dependable Systems
- RAID conferneces
- ACM KDD
- ACM Modeling, Analysis and Simulation Conference

- ACM Computer Architecture Conference
- ACM Computer and Communications Security
- Journal of Intelligent Information Systems
- Journal of Parallel and Distributed Computing
- International Journal of Tools with AI
- NSF and NSF PYI proposals in the area of Knowledge and Data Base Systems, and Computer Architectures 1987-1994
- NSF Panels on Security research and Expeditions proposals
- International Conference on Parallel Processing,
- 1988 International Conference on Fifth Generation Computing Tokyo, Japan, 1992
- AAAI Conference,
- RIDE Workshop
- ISMIS Conference,
- KDD Conference
- Parallel Computing Journal
- International Conference on Machine Learning

Honors and Awards

- Measuring the Human Factor of Cyber Security, (with B. Bowen and R. Devarajan), Proc. IEEE Homeland Security Technology Conference, IEEE HST, 2011.(Best Paper award)
- A Quantitative Analysis of the Insecurity of Embedded Network Devices: Results of a Wide-Area Scan, Ang Cui and Salvatore J. Stolfo, Annual Computer Security Applications Conference, ACSAC, 2010. (Best Paper Award)
- Bright Idea on Information Technology Award, "A link mining algorithm for earnings forecast and trading", Stillman Business School of Seton Hall University and the New Jersey Business and Industry Association NJPRO Foundation
- Managing Insider Security Threats Workshop (MIST), 2010, Best Paper
- IEEE Security and Privacy, Oakland Conference, Most Influential paper 2010
- Usenix Best Freenix Track Paper Award, MEF: Malicious Email Filter, June 2001
- Service Award, ACM, Program Co-Chair KDD2000, Aug 2000.
- Best Applied Research Award, Mining in a Data-flow Environment: Experience in Network Intrusion Detection, SIGKDD Int. Conference on Knowledge Discovery and Data Mining, Aug, 1999.
- Honorable Mention, Best Application Paper, KDD98 "Mining Audit Data to Build Intrusion Detection Models", New York, August, 1998.
- Runner Up Best Paper Award, KDD97, "JAM: Java Agents for Meta-Learning", Newport Beach, CA, August, 1997.
- Senior Member IEEE, 1996.
- IBM Faculty Career Development Award, $60,000 for two year period.
- Who's Who in the East, 1986.
- American Men and Women of Science, 1986, 1997.

Newsworthy Items in Popular Press or Periodicals

- Hacking Cisco IP Phones
  http://bits.blogs.nytimes.com/2013/02/05/a-guide-to-spying-on-cisco-phone-calls/
  http://redtape.nbcnews.com/_news/2013/01/04/16328998-popular-office-phones-vulnerable-to-eavesdropping-hack-researchers-say?lite&ocid=msnhp&pos=1
  http://www.washingtonpost.com/world/national-security/to-thwart-hackers-firms-salting-their-servers-with-fake-data/2013/01/02/3ce00712-4afa-11e2-9a42-d1ce6d0ed278_story.html?hpid=z4
- Symbiote Technology, Scientific American, Nov 2012, https://www.scientificamerican.com/article.cfm?id=new-symbiote-may-protect-microchips-from-cyberattack&WT.mc_id=SA_sharetool_StumbleUpon
- Hacking attacks on printers still not being taken seriously, The Guardian, July 23, 2012, http://www.guardian.co.uk/technology/2012/jul/23/hacking-attack-printers

- Feds Look to Fight Leaks With 'Fog of Disinformation', Wired Magazine, July 3, 2012, http://www.wired.com/dangerroom/2012/07/fog-computing/2/
- *http://redtape.nbcnews.com/_news/2013/01/04/16328998-popular-office-phones-vulnerable-to-eavesdropping-hack-researchers-say?lite&ocid=msnhp&pos=11*
- *Active Authentication and decoy technology*
- *http://www.nytimes.com/2012/03/18/business/seeking-ways-to-make-computer-passwords-unnecessary.html?partner=rss&emc=rss*
- *http://www.washingtonpost.com/world/national-security/to-thwart-hackers-firms-salting-their-servers-with-fake-data/2013/01/02/3ce00712-4afa-11e2-9a42-d1ce6d0ed278_story.html?hpid=z4*
- *NPR Radio interview, Marketplace Tech Report, HP vulnerability, Nov 2011.*
- *New York Times, Business section, Digital Domain, Seeking Ways to Make Passwords Unnecessary, March 17, 2012, http://www.nytimes.com/2012/03/18/business/seeking-ways-to-make-computer-passwords-unnecessary.html?partner=rss&emc=rss*
- *NPR Radio interview, Marketplace Tech Report, on research to replace password, Decoy technology, March 2012*
- *HP Printer Flaws, MSNBC, http://redtape.msnbc.msn.com/_news/2011/11/29/9076395-exclusive-millions-of-printers-open-to-devastating-hack-attack-researchers-say*
- Wired Magazine, interview concerning Decoy Technology. Nov 2011 http://www.wired.com/dangerroom/2011/11/darpa-trap-wikileaks/
- *Time Magazine*, "Cyberdefense", November 10, 2003.
- *Trusted Information Systems Magazine*, "The JAM Project", March 1998.
- *Associated Press Newswire*, Egs. The Bergen Record pp. E3, Staten Island Advance, "ATT accused of High-Tech Piracy", October 17, 1991.
- *New York Times*, "Scientists Bet on New Design", Science Times Section, pp. C1, Tuesday, October 23, 1984.
- *Manhattan Inc*, "Silicon Island*",* pp. 107-116, March 1986.

Issued Patents

1. 4,860,201, Issued August 22 1989-Binary tree parallel processor
2. PCT Issued-1989-Binary tree parallel processor
3. 4,843,540, Issued June 27, 1989-Parallel processing method
4. PCT Issued, Issued 1989-Parallel processing method
5. 5,363,473, Issued Nov. 8, 1994-Incremental update process and apparatus for an inference system
6. 5,563,783, Issued Oct 8, 1996-Method and system for securities pool allocation
7. 5,497,486, Issued March 5, 1996-Method of merging large databases in parallel
8. 5,668,897, Issued Sep 16, 1997-Method and apparatus for imaging, image processing and data compression merge/purge techniques for document image databases
9. 5,748,780, Issued May 5, 1998-Method and apparatus for imaging, image processing and data compression
10. 5,717,915, Issued Feb 10, 1998-Method of merging large databases in parallel
11. 5,920,848, Issued July 6, 1999-Method and system for using intelligent agents for financial transactions, services, accounting, and advice
12. 7,069,249, Issued Jun 27, 2006, Electronic purchase of goods over a communications network including physical delivery while securing private and personal information of the purchasing party
13. 7,162,741, Issued Jan 9, 2007, System and Methods for Intrusion Detection with Dynamic Window Sizes.
14. 7,225,343, Issued May 29, 2007, System and methods for adaptive model generation for detecting intrusions in computer systems

15. 7,277,961, Issued Oct 2, 2007, Method and System for Obscuring User Access Patterns Feb Using a Buffer Memory.
16. 7,424,619, Issued September 9, 2008, System and methods for anomaly detection and adaptive learning.
17. 7,448,084, Issued November 4, 2008, System and methods for detecting intrusions in a computer system by monitoring operating system registry accesses.
18 7,487,544 Issued February 3, 2009, System and methods for detection of new malicious executables
19 7,536,360 B2, Issued May 19, 2009, Electronic Purchase of Goods Over a Communications Network including Physical Delivery While Securing Private and Personal Information of the Purchasing party,
20 7,639,714, Issued Dec 29, 2009 , Apparatus method and medium for detecting payload anomaly using n-gram distribution of normal data
21 7,657,935, Issued Feb 2, 2010, System and methods for detecting malicious email transmission
22 7,752,665, Issued July 6, 2010, Detecting Probes and scans over high-bandwidth, long-term incomplete network traffic information using limited memory
23 7,779,463, Issued August 17, 2010, Systems and methods for correlating and distributing intrusion alert information among collaborating computer systems.
24 7,784,097, Issued Aug 24, 2010, Systems and methods for correlating and distributing intrusion alert information among collaborating computer systems
25 7,818,797, Issued Oct. 19, 2010, Methods for Cost-Sensitive Modeling for Intrusion Detection and Response.
26 7,913,306, Issued Mar 22, 2011, System and Methods for detecting Intrusions in a computer system by monitoring operating system registry accesses.
27 7,962,798, Methods, systems and media for software self-healing, June 14, 2011.
28 7,979,907, Effective Method for Detecting Malicious Binary Programs, July 12, 2011.
29 Method and System for Processing Recurrent Consumer Transactions, May 5, 2002 pub date, Application (W0/2002/041224), Notice of Allowance April 28, 2011, Issued August 9, 2011.
30 8,074,115, Methods, media and systems for detecting anomalous program executions, December 6, 2011
31 8,239,687, , Apparatus method and medium for tracing the original of network transmissions using n-gram distribution of data, Issued August 7, 2012.
32 8,381,295, Systems and methods for correlating and distributing intrusion alert information among collaborating computer systems, App no. 10/864,226, notice of allowance, Issued February 19, 2013.
33 8,135,994, Methods, media, and systems for detecting an anomalous sequence of function calls, Issued March 13, 2013.
34 8,407,160, Systems, methods, and media for generating sanitized data, sanitizing anomaly detection models, and/or generating sanitized anomaly detection models, Issued March 26, 2013.
35 8,407,785, Systems, methods, and media protecting a digital data processing device from attack, Issued March 26, 2013.
36 8,443,441, System and Methods for Detecting Malicious Email Transmission, May 14, 2013.

37 8,448,242, Systems, methods and media for outputting data based upon anomaly detection . May 21, 2013.
38 20100077483, Notice of allowance Feb 2013, Methods, Ssystems, and Media For Baiting Inside Attackers.
39 8,528,091, Methods, systems, and media for detecting covert malware, September 3, 2013.
40 8,544,087, Methods of unsupervised anomaly detection using a geometric framework, September 24, 2013.
41 8,601,322, Methods, media and systems for detecting anomalous program executions, December 3, 2013.
42 8,667,588, Systems and methods for correlating and distributing intrusion alert information among collaborating computer systems, March 4, 2014.
43 8,694,833, Methods, media, and systems for detecting an anomalous sequence of function calls, April 8, 2014.
44 8,763,103, Systems and methods for inhibiting attacks on applications, June 24, 2014.
45 8,769,684, Methods, systems, and media for masquerade attack detection by monitoring computer user behavior, July 1, 2014.
46 8,819,825, Systems, methods, and media for generating bait information for trap-based defenses, August 26, 2014.
47 8,844,033, Systems, methods, and media for detecting network anomalies using a trained probabilistic model, September 23, 2014.

Published Patent Applications

1 20100153785 METHODS, MEDIA, AND SYSTEMS FOR DETECTING AN ANOMALOUS SEQUENCE OF FUNCTION CALLS
2 20100146615 Systems and Methods for Inhibiting Attacks on Applications
3 20100077483 METHODS, SYSTEMS, AND MEDIA FOR BAITING INSIDE ATTACKERS
4 20100064369 METHODS, MEDIA, AND SYSTEMS FOR DETECTING ATTACK ON A DIGITAL PROCESSING DEVICE
5 20100064368 Systems, Methods, and Media for Outputting a Dataset Based Upon Anomaly Detection
6 20100054278 APPARATUS METHOD AND MEDIUM FOR DETECTING PAYLOAD ANOMALY USING N-GRAM DISTRIBUTION OF NORMAL DATA
7 20100023810 METHODS, MEDIA AND SYSTEMS FOR DETECTING ANOMALOUS PROGRAM EXECUTIONS
8 20100011243 Methods, systems and media for software self-healing
9 20090254992 SYSTEMS AND METHODS FOR DETECTION OF NEW MALICIOUS EXECUTABLES
10 20090241191 SYSTEMS, METHODS, AND MEDIA FOR GENERATING BAIT INFORMATION FOR TRAP-BASED DEFENSES
11 20090222922 SYSTEMS, METHODS, AND MEDIA PROTECTING A DIGITAL DATA PROCESSING DEVICE FROM ATTACK
12 20090193293 Systems, Methods, and Media for Outputting Data Based Upon Anomaly Detection
13 20090083855 System and methods for detecting intrusions in a computer system by monitoring operating system registry accesses
14 20080262985 SYSTEMS, METHODS, AND MEDIA FOR GENERATING SANITIZED DATA, SANITIZING ANOMALY DETECTION MODELS, AND/OR GENERATING SANITIZED ANOMALY DETECTION MODELS
15 20070239999 Systems and methods for adaptive model generation for detecting intrusions in computer systems
16 20070050708 Systems and methods for content extraction

17 20060247982 Electronic purchase of goods over a communications network including physical delivery while securing private and personal information of the purchasing party
18 20060178994 Method and system for private shipping to anonymous users of a computer network
19 20060015630 Apparatus method and medium for identifying files using n-gram distribution of data
20 20050281291 Apparatus method and medium for detecting payload anomaly using n-gram distribution of normal data
21 20050265331 Apparatus method and medium for tracing the origin of network transmissions using n-gram distribution of data
22 20050257264 Systems and methods for correlating and distributing intrusion alert information among collaborating computer systems
23 20040205474 System and methods for intrusion detection with dynamic window sizes
24 20040002903 Electronic purchase of goods over a communications network including physical delivery while securing private and personal information of the purchasing party
25 20030167402 System and methods for detecting malicious email transmission
26 20030065926 System and methods for detection of new malicious executables
27 20010044785 Method and system for private shipping to anonymous users of a computer network

Copyright Software - US Registered

1. PPL/M Kernel, Reg. No. TX 3-637-153, February, 1994, licensed to Fifth Generation Computer Corp.
2. DADO C and Parallel C Header Files, Reg. No. TXu 593-187, January 1994, licensed to Fifth Generation Computer Corp.
3. DADO C Kernel and Parallel Processing Library, Reg. No. TXu 593-186, January 1994, licensed to Fifth Generation Computer Corp.
4. Parallel C Preprocessor, Compiler, Kernel, and Utility Program Code, Reg. No. TXu 593-188, January 1994, licensed to Fifth Generation Computer Corp.

Copyright User's Guides

1. The DataCleanser DataBlade Module - User's Guide, (with Joyce Simmon, Mauricio Hernandez and William White), part No. XX, Informix Software Publishers, 1997.

Formal Workshop Reports

1. Report on the AAAI 97 Workshop on Fraud and Risk Management, (with T. Fawcett, I. Haimowitz, F. Provost), AAAI, AI Magazine, Spring 1998.
2. Towards the Digital Government of the 21st Century, A Report from the Workshop on R&D Opportunities in Federal Information Services, (with Herbert Schorr), June, 1997.

Formal Government Reports

MINESTRONE, Salvatore Stolfo, Angelos D. Keromytis, Junfeng Yang, Dimitris Geneiatakis, Michalis Polychronakis, Georgios Portokalidis, Kangkook Jee, and Vasileios P. Kemerlis Columbia University, Angelos Stavrou and Dan Fleck, George Mason University, Nathan Evens, Matthew Elder, and Azzedine Benameur Symantec, AFRL-RY-WP-TR-2015-0002, AIR FORCE RESEARCH LABORATORY, SENSORS DIRECTORATE, WRIGHT-PATTERSON AIR FORCE BASE, OH 45433-7320, AIR FORCE MATERIEL COMMAND, UNITED STATES AIR FORCE, January 2015.

Books and Journal Issues (Edited)

1. *Proceedings 16th International Symposium, RAID 2013, (Stolfo, Salvatore; Stavrou, Angelos; Wright, Charles (Eds.),) Rodney Bay, St. Lucia, (ISBN 978-3-642-41283-7) October 23-25, 2013.*
2. *IEEE Security and Privacy Special Issue on the Science of Security*, co-Editor, May 2011.

3. *IEEE Security and Privacy Special Issue on Privacy-Preserving Sharing of Sensitive Information*, co-Editor, 2009-2010.
4. *IEEE Security and Privacy Special Issue on Insider Threat*, co-Editor, 2009.
5. *Insider Attack and Cyber Security: Beyond the Hacker*, (Stolfo, Bellovin S, Hershkop, Keromytis A, Sinclair S, Smith S, Eds.) ISBN-13: 978-0-387-77321-6, Springer, 2008.
6. *Proceedings of KDD2000 The Sixth ACM SIGKDD*, International Conference on Knowledge Discovery And Data Mining, (with R. Ramakrishnan, R. Bayardo, and I. Parsa), Association for Computing Machinery (ACM), ISBN: 1-58113-233-6, Boston, MA, August, 2000.
7. *Machine Learning Journal*, Special Issue on Integrating Multiple Learned Models for Improving and Scaling Machine Learning Algorithms, Volume 36, Number 1&2, 1999.

Book Chapters - Peer Refereed

1. Symbiotes and Defensive Mutualism: Moving Target Defense, (with A. Cui),, in *Moving Target Defense, Creating Asymmetric Uncertainty for Cyber Threats*, (Jajodia, Ed.), ISBN: 978-1-4614-0976-2,Springer, 2011.
2. Insider Threats, (with B. Bowen and M. Ben Salem), in *Encyclopedia of Cryptography and Security* (2nd Ed.), (Jajodia, Ed.), Springer, 2011.
3. Monitoring Technologies for Mitigating Insider Threats, (with B. Bowen, M. Ben Salem, and A. D. Keromytis), in *Insider Threats in Cyber Security*, ISBN: 978-1-4419-7132-6,Springer, 2010.
4. Automated Social Hierarchy Detection through Email Network Analysis, (with R. Rowe, G. Creamer, and S. Hershkop), revised papers of the Web Mining and Social Network Analysis Workshop on International Conference on Knowledge Discovery and Data Mining (KDD), Lecture Notes in Computer Science, Springer-Verlag, 2008.
5. Towards Stealthy Malware Detection, (with K. Wang, and W. Li), *Malware Detection Book*, Springer Verlag, (Jha, Christodorescu, Wang, Eds.), 2006.
6. Cost-Sensitive Modeling for Intrusion Detection, (with W. Lee, W. Fan, and M. Miller), in *Machine Learning and Data Mining for Computer Security*, (M. Maloof, Ed.), Springer, 2005. (ISBN-10: 1-84628-029-X)
7. Collaborative Security, in *The Black Book of Corporate Security*, Larstan Pub., ISBN: 0-9764266-1-7, November, 2004.
8. A Geometric Framework for Unsupervised Anomaly Detection Detecting Intrusions in Unlabeled Data. (with E. Eskin, A. Arnold, M. Prerau, and L. Portnoy), in *Data Mining for Security Applications,* (Jajodia and Barbara, Eds.) Kluwer, 2002.
9. Adaptive Model Generation: An Architecture for the Deployment of Data Mining-based Intrusion Detection Systems, (with A. Honig, A. Howard, and E. Eskin), in *Data Mining for Security Applications,* (Jajodia and Barbara, Eds.) Kluwer, 2002.
10. Meta-learning in Distributed Data Mining Systems: Issues and Approaches, (with A. Prodromidis, and P. Chan), in *Advances in Distributed and Parallel Knowledge Discovery*, (Kargupta and Chan, Eds.), AAAI/MIT Press, 2000, pp. 81-114.
11. Algorithms for Mining System Audit Data, (with W. Lee and K. Mok), in *Data Mining, Rough Sets and Granular Computing*, (T. Y. Lin, Y. Yao, and L.A. Zadeh, Eds.), Physica-Verlag, 2002.
12. A Parallel and Distributed Environment for Database Rule Processing, Open Problems and Future Directions, (with H. Dewan, D. Ohsie, and M. Hernandez), in *Emerging Trends in Database and Knowledge-based Machines*, IEEE Press, 1995 (ISBN: 0-8186-6552-1).
13. System Reorganization and Load Balancing of Parallel Database Rule Processing, (with H. Dewan), in *Methodologies for Intelligent Systems, Lecture Notes in Artificial Intelligence*, Vol. 689, (J. Komorowsky and Z. Ras, Eds.), Springer-Verlag, 1993, pp. 186-197.
14. DADO: A Parallel Computer for Artificial Intelligence, in *Encyclopedia of Artificial Intelligence, Second Edition* 1991, John Wiley & Sons, New York. pp. 414-417.
15. Let's Stop the Dust from Collecting on OPS5, (with R. Mills, A. Pasik and M. VanBiema), in *Concepts and Characteristics of Knowledge-based Systems*, (Tokoro, Anzai and Yonezawa, Eds.), North-Holland, 1989, pp. 37-58.
16. DADO: A Parallel Computer for Artificial Intelligence, *Encyclopedia of Artificial Intelligence, First Edition*, 1986, John Wiley & Sons, New York, pp. 227-229.
17. The Do-Loop Considered Harmful in Production System Programming (with M. van Biema and D. Miranker), in *Expert Database Systems*, (L. Kerschberg, Editor), Benjamin/Cummings, 1986, pp. 177-190.
18. A Simple Preprocessing Scheme to Extract and Balance Implicit Parallelism in the Concurrent Match of Production Rules, in *Fifth Generation Computer Architectures*, (Woods, Ed.), North-Holland, 1986, pp. 55-66.

19. DADO: A Parallel Processor for Expert Systems (with D. Miranker), in *Computers for Artificial Intelligence Applications*, (Wah and Li, Eds.), IEEE Computer Society Press, No. 706, 1986, pp. 473-481.
20. DADO: A Tree-Structured Architecture for Artificial Intelligence Computation (with D. Miranker), (invited article), *Annual Review of Computer Science*, Vol. 1, 1986, William Kaufmann, Inc. pp. 1-18.
21. DADO: A Parallel Processor for Expert Systems (with D. Miranker), in *Tutorial on Advanced Computer Architecture*, (D. Agrawal, Ed.), IEEE Computer Society Press, No. 667, 1986, pp. 364-372.

Journal and Periodical Publications - Refereed and Accepted

1. Bait and Snitch: Defending Computer Systems with Decoys, with (J. Voris and A. D. Keromytis), (T.Saadawi, L. Jordan, editors), Cyber Infrastructure Protection, Volume 3, SSI, January 2014.
2. Revisiting the Myth of Cisco IOS Diversity: Recent Advances in Reliable Shellcode Design, (with A. Cui and M. Costello),), in Information Management & Computer Security (IMCS). 21.2, to appear 2014. Does profiling make us more secure? Pfleeger, S.L., Rogers, M., Bashir, M., Caine, K., Caputo, D., Losavio, M., Stolfo, S. 2012, IEEE Security and Privacy 10 (4) , art. no. 6265096 , pp. 10-15.
3. Usable Secure Private Search, (with B. Vo, M. Raykova, A Cui, T. Malkin, and S. Bellovin), *IEEE Security and Privacy*, 2011.
4. A System for Generating and Injecting Indistinguishable Network Decoys, (with Brian M. Bowen, Vasileios P. Kemerlis, Pratap Prabhu, Angelos D. Keromytis), *Journal of Computer Security (JCS*), 2011.
5. Modeling User Search Behavior for Masquerade Detection, (with M. Ben Salem), *The Innovator,* (FS Roundtable/BITS), Volume 4, February 2011.
6. Measuring Security, (with S. Bellovin and D. Evans), *On the Horizon* (V. Varadharajan and F. Cohen, Eds.), IEEE Security and Privacy Magazine Special Issue on the Science of Security, 2011.
7. A Comparison of One-Class Bag-of-Words User Behavior Modeling Techniques for Masquerade Detection, (with M. Ben Salem), in Security and Communication Networks Journal, (Bertino, Ed.), Willey, (to appear 2011).
8. Detecting Masqueraders: A Comparison of One-Class Bag-of-Word User Behavior Modeling Techniques, M. Ben Salem and S. J. Stolfo, *Security and Communication Networks* Journal, 2010:00-1=11, 2010.
9. Insider Threats, S. Stolfo, B. Bowen and M. Ben Salem, in *Encyclopedia of Cryptography and Security* (2nd ed.), (Eds. Tilborg and Jajodia), 2011.
10. Ethics in Security Vulnerability Research, (with A. Matwyshyn, A. Cui, and A. D. Keromytis), *IEEE Security and Privacy,* Basic Training (R. Ford and D. Frincke, Eds.), Spring 2010.
11. On the Infeasibility of Modeling Polymorphic Shellcode: Re-thinking the Role of Learning in Intrusion Detection Systems, (with Y. Song and A.D. Keromytis), *Machine Learning Journal*, Special Issue on Adversarial Learning, 2010.
12. Addressing the Insider Threat, (with S. Pfleeger), *IEEE Security and Privacy Special Issue on Insider Threats*, (S. Pfleeger and Stolfo, Editors), Volume 7, Number 6, November/December 2009.
13. Designing Host and Network Sensors to Mitigate the Insider Threat, (with B. Bowen, M. Ben Salem, S. Hershkop, A. D. Keromytis), *IEEE Security and Privacy Special Issue on Insider Threats*, Volume 7, Number 6, November/December 2009.
14. Segmentation and Automated Social Hierarchy Detection through Email Network Analysis, (with R. Rowe, G. Creamer and S. Hershkop), in Zhang et al. eds. *Advances in Web Mining and Web Usage Analysis* - 9th WEBKDD and 1st SNA-KDD Workshop at KDD 2007, Lecture Notes in Computer Science, Springer-Verlag, 2008.
15. A Comparative Evaluation of Two Algorithms for Windows Registry Anomaly Detection, (with F. Apap, E. Eskin, K. Heller, S. Hershkop, and A. Honig and K. Svore), *Journal of Computer Security*, 2006.
16. Behavior-based Modeling and its Application to Email Analysis, (with S. Hershkop, A. Hu, O. Mineskern, and K. Wang), ACM *Transaction on Internet Technology*, 2006.
17. 10 Challenging Problems in Data Mining Research, Yang Q. and Wu X (Contributors: Pedro Domingos, Charles Elkan, Johannes Gehrke, Jiawei Han, David Heckerman, Daniel Keim, Jiming Liu, David Madigan, Gregory Piatetsky-Shapiro, Vijay V. Raghavan, Rajeev Rastogi, Salvatore J. Stolfo, Alexander Tuzhilin, and Benjamin W. Wah), *International Journal of Information Technology & Decision Making*, Vol. 5, No. 4, 2006, 597-604.
18. An Email Worm Vaccine Architecture**,** (with S. Sidiroglou, J. Ioannidis, A. D. Keromytis), *Lecture Notes in Computer Science*, Springer-Verlag GmbH, Volume 3439, 2005.
19. Worm and Attack Early Warning: Piercing Stealthy Reconnaissance, On the Horizon, IEEE Privacy and Security, May/June, 2004.
20. Using Artificial Anomalies to Detect Known and Unknown Network Intrusions, (with W. Fan, M. Miller, W. Lee and P. Chan), *Knowledge And Information Systems Journal*, (Springer-Verlag), 2002.

21. Toward Cost-Sensitive Modeling for Intrusion Detection, (with W. Lee,. W. Fan, M. Miller and E.Zadok), *Journal of Computer Security*, Vol. 10, Numbers 1,2, 2002.
22. Cost Complexity-based Pruning of Ensemble Classifiers, (with A. Prodromidis), *Journal on Distributed and Parallel KDD*, Special Issue on Knowledge and Information Systems, 2000.
23. Adaptive Model Generation for Intrusion Detection, (with E. Eskin, M. Miller, Z. Zhang, G. Yi, L. Wei-Ang), *IEEE Journal of Computer Security*, 2000.
24. A Framework for Constructing Features and Models for Intrusion Detection Systems, (with W. Lee), *ACM Transactions on Information and System Security*, TISSEC, Vol 3, Number 4, November, 2000.
25. Distributed Data Mining in Credit Card Fraud Detection, (with P. Chan, W. Fan, A. Prodromidis*), IEEE Intelligent Systems*, Vol. 14, No. 6, 1999.
26. Adaptive Intrusion Detection: a Data Mining Approach, (with W. Lee and K. Mok*), Artificial Intelligence Review,* Volume 14, No. 6, Kluwer Academic Publishers, 2000, pp. 533-567.
27. Towards the Digital Government of the 21st Century, (with H. Schorr), *Communications of the ACM, CACM*, November, 1998.
28. Scalability of Hierarchical Meta-Learning on Partitioned Data, (with P. Chan*), Journal of Data Mining and Knowledge Discovery*, (U. Fayad, Ed.), Kluwer, (submitted, under revision).
29. Real-world Data is Dirty: Data Cleansing and the Merge/Purge Problem, (with M. Hernandez), *Journal of Data Mining and Knowledge Discovery*, (U. Fayad, Ed.), Kluwer, No. 2, 1998, pp. 9-37.
30. On the Accuracy of Meta-learning for Scalable Data Mining, (with P. Chan), *Journal of Intelligent Information Systems*, (L. Kerschberg, Ed.), Kluwer, No 8, 1997, pp. 5-29.
31. Scalable Expert Database Systems, (with H. Dewan), *Journal of Parallel and Distributed Computing*, Special Issue on Scalability, (Kumar, Ed.), Vol. 22, No. 3, September, 1994, pp. 506-522.
32. High Performance Computing and Communications for Grand Challenge Applications: Computer Vision, Speech and Natural Language Processing, and Artificial Intelligence, (with B. Wah, T. Huang, A. Joshi, D. Moldovan, J. Aloimonos, R. Bajcsy, D. Ballard, D. DeGroot, K. DeJong, C. Dyer, S. Fahlman, R. Grishman, L. Hirschman, R. Korf, S. Levinson, D. Miranker, N. Morgan, S. Nirenburg, T. Poggio, E. Riseman, C. Stanfill, S. Stolfo, S. Tanimoto, C. Weems) *IEEE Transactions on Knowledge and Data Engineering*, (B. Wah, Ed.) Vol. 5, No. 1, Feb. 1993.
33. Incremental Database Rule Processing in PARADISER, (with H. Dewan, D. Ohsie, S. Da Silva and O. Wolfson), *Journal of Intelligent Information Systems*, 1992, Vol 1:2, pp. 177-209.
34. PARULEL: Parallel Rule Processing Using Meta Rules for Redaction, (with O. Wolfson, P. Chan, H. Dewan and D. Ohsie), *Journal of Parallel and Distributed Computing*, Vol 13, No.4, December 1991, pp. 366-382.
35. Initial Performance of the Dado2 Prototype, *IEEE Computer Magazine*, January, 1987, pp. 75-84.
36. The DADO Production System Machine (with D. Miranker), *Journal of Parallel and Distributed Computing*, Academic Press, 1986.
37. Parallelism in New Generation Computing, (transcribed invitational panel discussion), *ICOT Journal*, Vol. 1, No. 7, (Aizawa, Ed.), 1985, pp. 12-35.
38. The Application of AI and DADO Parallel Processor Technology to Future Unmanned Vehicle Systems, (with S. Alterman), in Unmanned Systems, *The Magazine of the Association for Unmanned Vehicle Systems*, Vol. 4, No. 2, 1985, pp. 10-19.
39. Is CAD/CAM Ready for AI?, *Journal of Applied Finite Elements and CAD/CAM*, Vol. 1, 1985, pp. 1-12.
40. Learning Control of Production Systems, Journal of Cognition and Brain Theory, Vol. 7, No. 1,1984, Erlbaum, pp. 61-88.
41. The Non-Von Data Base Machine: A Brief Overview (with D. Shaw, H. Ibrahim, B. Hillyer, G. Wiederhold, and J. Andrews), *Database Engineering*, Vol. 4, 1981, IEEE, pp. 41-52.

Conference and Symposia Proceedings - Refereed

1. Improving Readiness for Enterprise Migration to the Cloud, J. Jermyn, J. Hwang, K. Bai, M. Vukovic, N. Anerousis, and S. J. Stolfo, Proc. Of the Middleware Industry Track, Middleware 2014.
2. Unsupervised Anomaly-based Malware Detection using Hardware Features Adrian Tang, Simha Sethumadhavan, and Salvatore Stolfo (Columbia University), RAID 2014.
3. Measuring Drive-by Download Defense in Depth Nathaniel Boggs, Senyao Du, and Salvatore J. Stolfo (Columbia University), RAID 2014.
4. Synthetic Data Generation and Defense in Depth Measurement of Web Applications Nathaniel Boggs, Hang Zhao, Senyao Du, and Salvatore J. Stolfo (Columbia University), RAID 2014.

5. On the Feasibility of Online Malware Detection with Performance Counters (with J. Demme, M. Maycock, J. Schmitz, A. Tang, A. Waksman, and S. Sethumadhavan), Proc. 40th International Symposium on Computer Architecture (ISCA40), Isreal, 2013.
6. On the Use of Decoy Applications for Continuous Authentication on Mobile Devices, M. Ben Salem, J. Voris and S. J. Stolfo, Who are you? Adventures in Authentication, WAY 2014.
7. When Firmware Modifications Attack: A Case Study of Embedded Exploitation, (with A. Cui and M. Costello), Proceedings Annual Network & Distributed System Security Symposium (NDSS) 2013.
8. Software Decoys for Insider Threats, Younghee Park and Salvatore J Stolfo, Proceedings ACM Symposium on Information, Computer and Communications Security (ASIACCS), 2012.
9. Measuring the Human Factor of Cyber Security, (with B. Bowen and R. Devarajan), Proc. IEEE Homeland Security Technology Conference, IEEE HST, 2011.(Best Paper award)
10. Behavior-based Network Traffic Synthesis, (w. Y. Song), Proc. IEEE Homeland Security Technology Conference, IEEE HST, 2011.
11. From Prey To Hunter: Transforming Legacy Embedded Devices Into Exploitation Sensor Grids, (with A. Cui and J. Kataria), Proc. of the Annual Computer Security Applications Conference, ACSAC, 2011.
12. Cross-domain Collaborative Anomaly Detection: So Far Yet So Close, (with N. Boggs, S. Hiremagalore, and A. Stavrou), Proc. of the International Conference on Recent Advances in Intrusion Detection (RAID), September 2011.
13. Masquerade Attack Detection Using a Search Behavior Modeling Approach, (with M. Ben Salem), Proc. of the International Conference on Recent Advances in Intrusion Detection (RAID), September 2011.
14. Defending Legacy Embedded Systems with Software Symbiotes, (with A. Cui), Proc. of the International Conference on Recent Advances in Intrusion Detection (RAID), September 2011.
15. Decoy Document Deployment for Effective Masquerade Attack Detection, (with M. Ben Salem), Proceedings 8th Conference on Detection of Intrusions and Malware and Vulnerability Assessment (DIMVA), 2011.
16. A Quantitative Analysis of the Insecurity of Embedded Network Devices: Results of a Wide-Area Scan, Ang Cui and Salvatore J. Stolfo, Annual Computer Security Applications Conference, ACSAC, 2010. (Best Paper Award)
17. Botswindler: Tamper Resistant Injection of Believable Decoys in VM-Based Hosts for Crimeware Detection, Brian M. Bowen, Pratap Prabhu, Vasileios P. Kemerlis, Stelios Sidiroglou, Angelos D. Keromytis, and Salvatore J. Stolfo, RAID 2010.
18. Experimental Results of Cross-Site Exchange of Content Anomaly Detector Alerts, Salvatore J. Stolfo, Nathaniel Boggs, Angelos Stavrou and Sharath Hiremagalore, IEEE Homeland Security Technology Conference, (IEEE HST), 2010.
19. A Network Access Control Mechanism Based on Behavior Profiles, (with V. Frias-Martinez, J. Sherrick, A. D. Keromytis), Proc. Annual Computer Security Applications Conference, ACSAC 2009, Dec, 2009.
20. BARTER: Behavior Profile Exchange for Behavior-Based Admission and Access Control in MANETs, (with V. Frias-Martinez, J. Sherrick, A. D. Keromytis), Proc. 5th Int, Conference on Information Systems Security (ICISS 2009), 2009.
21. Baiting Inside Attackers Using Decoy Documents (with Brian Bowen, Shlomo Herkshop, Angelos D Keromytis), Proc. 5th International ICST Conference on Security and Privacy in Communication Networks, SecureComm, 2009.
22. Adaptive Anomaly Detection via Self-Calibration and Dynamic Updating, (with G. Cretu-Ciocarlie, A. Stavrou and M. Locasto), Proc. *Int. Conf. on Recent Advanced in Intrusion Detection, RAID09*, 2009.
23. Spectrogram: A Mixture-of-Markov-Chains Model for Anomaly Detection in Web-Traffic, (with. Y. Song, A. Keromytis), Proc. *Network and IT Security Symposium*, (NDSS 09), 2009.
24. Behavior-Profile Clustering For False Alert Reduction in Anomaly Detection Sensors, (with V. Frias-Martinez and A. D. Keromytis), Proc. *Annual Computer Security Applications Conference*, (ACSAC) 2008.
25. Behavior-Based Network Access Control: A Proof-of-Concept , (with V Frias-Martinez, and A. D. Keromytis), *In the Proceedings of the 11th Information Security Conference (ISC), 2008.*
26. Casting out Demons: Sanitizing Training Data for Anomaly Sensors, (with G. Cretu, A. Stavrou, M. Locasto, and A. Keromytis), *IEEE Security and Privacy*, (Oakland), 2008.
27. On the Infeasibility of Modeling Polymorphic Shellcode for Signature Detection, (with Y. Song, M. Locasto, A. Stavrou, A. Keromytis), Proc. *ACM Computer and Communications Security (CCS),* 2007.
28. A Study of Malcode-bearing Documents, (with Wei-Jen Li, Elli Androuloki and Angelos Stavrou), DIMVA 2007.
29. Data Sanitization: Improving the Forensic Utility of Anomaly Detection Systems, (with G. Cretu, A. Stavrou and A. Keromytis), HOTDEP 2007.
30. A Temporal Based Forensic Analysis of Electronic Communication, (with G. Creamer, and S. Hershkop), in Digital Government Proceedings, San Diego, CA, 2006.
31. A Link Mining Algorithm for Earnings Forecast Using Boosting <http://ssrn.com/abstract=938044> (with Germán Creamer), in Proceedings of the Link Analysis: Dynamics and Statistics of Large Networks, Workshop on International Conference on Knowledge Discovery and Data Mining (KDD), Philadelphia, 2006.

32. Privacy-Preserving Payload-Based Correlation for Accurate Malicious Traffic Detection" (with J. Parekh, Ke Wang) *In SIGCOMM Workshop on Large Scale Attack Defense 2006*
33. Anagram: A Content Anomaly Detector Resistant to Mimicry Attack, (with K. Wang and J. Parekh), Proc. *Int. Conf. on Recent Advanced in Intrusion Detection, RAID06*, Sept 2006 (CU Tech Report 020-06).
34. Verifying Genre-based Clustering Approach to Content Extraction", (with S. Gupta, H. Becker and G. Kaiser),*13th International World Wide Web Conference*, May 2006.
35. Intrusion and Anomaly Detection Model Exchange for Mobile Ad-Hoc Network, (with G. Cretu, J. Parekh, and K. Wang), *IEEE CCNC*, 2006.
36. Combining Email Models for False Positive Reduction, (with S. Hershkop), The Eleventh ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, KDD-05, 2005.
37. Anomalous Payload-based Worm Detection and Signature Generation, (with K. Wang and G. Cretu), Intl. Conference on Recent Advances in Intrusion Detection, RAID, 2005.
38. FLIPS: Hybrid Adaptive Intrusion Prevention, (with M. Locasto, K. Wang and A. Keromytis), Intl. Conference on Recent Advances in Intrusion Detection, RAID, 2005.
39. Extracting Context To Improve Accuracy For HTML Content Extraction**,** (with S. Gupta and G. Kaiser), Int. World Wide Web Conference, WWW 2005. (Best student paper award.)
40. An Email Worm Vaccine Architecture, (with S. Sidiroglou, J. Ioannidis, A. Keromytis), Lecture Notes (Springer) of First Information Security Practice and Experience Conference (ISPEC 2005).
41. Unsupervised Anomaly Detection in Computer Security and an Application to File System Access, (with L. Bui, S. Hershkop), ISMIS, 2005. (Invited)
42. Anomalous Payload-based Network Intrusion Detection, (with K. Wang), Recent Advances in Intrusion Detection, RAID-2004, France, 2004.
43. A Behavior-based Approach to Securing Email Systems, (with S. Hershkop, Ke Wang, O. Nimerkern and C.Hu) *"Mathematical Methods, Models and Architectures for Computer Networks Security"*, Proceedings published by Springer Verlag, Sept. 2003.
44. Citizen's Attitudes about Privacy While Accessing Government and Private Websites: Results of an Online Study, (with E. Johnson, T. Pavlicic and S. Jan), NSF Digital Government Conference, DG.O 2003, Boston, May 2003.
45. Behavior Profiling of Email, NSF/NIJ Symposium On Intelligence and Security Informatics, ISI 2003, Arizona, June, 2003.
46. Surveillance Detection in High Bandwidth Environments, (with S. Robertson, E. Siegel, M. Miller), DARPA DISCEX III, pp 130, April 2003.
47. EMT/MET: Systems for Modeling and Detecting Errant Email, (with S. Hershkop, K. Wang and O. Mineskern), DARPA DISCEX III, pp 290, April 2003.
48. Detecting Malicious Software by Monitoring Anomalous Windows Registry Accesses, (with F. Apap, A. Honig, S. Hershkop, E. Eskin), Recent Advanced in Intrusion Detection (RAID), 2002.
49. A Fully Distributed Framework for Cost-sensitive Data Mining, (with W. Fan, H Wang and P. Yu), Int. Conference on Distributed Computing Systems, ICDCS, Vienna, Austria, pp 445, 2002.
50. Progressive Modeling, (with W. Fan, H. Wang, P. Yu, S. Lo), Proceedings of the 22nd International Conference on Distributed Computing Systems (ICDCS'02), July 2-5, 2002, Vienna, Austria. IEEE Computer Society.
51. A Framework for Scalable Cost-sensitive Learning Based on Combining Probabilities and Benefits (with W. Fan, H. Wang and P. Yu), SIAM International Conference on Data Mining, Arlington, VA, 2002.
52. Ensemble-based Adaptive Instrsion Detection, (with W. Fan), SIAM International Conference on Data Mining, Arlington, VA, 2002.
53. Using Artificial Anomalies to Detect Known and Unknown Network Intrusions, (with W. Fan), IEEE 1st International Conference on Data Mining, 2001.
54. Real Time Data Mining-based Intrusion Detection, (with W. Lee, P. Chan, D. Fan, E. Eskin, M. Miller), 2nd DARPA Information Survivability Conference and Exposition (DISCEX II), 2001.
55. Data Mining Methods for the Detection of Malicious Executables, (with M. Schultz, E. Eskin, E. Zadok), IEEE Symposium on Security and Privacy, 2001.
56. MEF, Malicious Email Filter, A Unix Mail Filter that Detects Malicious Windows Executables, (with M. Schultz, E. Eskin), USENIX Technical Symposium FREENIX Track, 2001, (Best Student Paper Award).
57. A Data Mining and CIDF Based Approach for Detecting Novel and Distributed Intrusions, (with W. Lee, R. Nimbalkar, K. Yee, S. Patil, P. Desai, T. Tran), Proc. Conf. Research Advances in Intrusion Detection, RAID 2000.
58. A Multiple Model Cost-sensitive Approach for Intrusion Detection, (with W. Fan, W. Lee and M. Miller), European Conference on Machine Learning, 2000.

59. Cost-based Modeling for Fraud and Intrusion Detection: Results from the JAM Project, (with W. Fan, W. Lee, A. Prodromidis and P. Chan), Proc. DARPA Information Survivability Conference and Exposition, IEEE Computer Press, 2000.
60. Combining Knowledge Discovery and Knowledge Engineering to Build IDSs, (with W. Lee), In Proceedings of the 2nd International Workshop on Recent Advances in Intrusion Detection (RAID '99), 1999.
61. Mining in a Dataflow Environment: Experience in Network Intrusion Detection, (with. W. Lee and K. Mok), (Best Paper Award in Applied Research Category), In Proceedings of the 5th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining (KDD '99), San Diego, CA, August, 1999.
62. The Application of AdaBoost for Scalable, Distributed and On-line Learning, (with. W. Fan and J. Zhang), In Proceedings of the 5th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining (KDD '99), San Diego, CA, August, 1999
63. AdaCost: Misclassification cost-sensitive Boosting, (with W. Fan, J. Zhang and P. Chan), In Proceedings of Sixteenth International Conference on Machine Learning, Slovenia, pp. 99-105, 1999.
64. A Data Mining Framework for Building Intrusion Detection Models, (with W. Lee and K. Mok), 1999 IEEE Symposium on Security and Privacy, 1999.
65. Pruning Meta-Classifiers in a Distributed Data Mining System, (with A. Prodromidis), NIT'98 Conference (New Information Technology), Athens, Greece, 1998.
66. Mining Audit Data to Build Intrusion Detection Models, (with W. Lee and K. Mok), Int. Conf. On Knowledge Discovery in Databases and Data Mining, KDD98, (honorable mention, best application paper), 1998, pp. 66-72.
67. Towards Scalable Learning with Non-uniform Class and Cost Distributions: A Case Study in Credit Card Fraud Detection, (with P. Chan), Int. Conf. On Knowledge Discovery in Databases and Data Mining, KDD98, 1998, pp. 164-168.
68. Mining databases with different schemas: Integrating incompatible classifiers, (with A. Prodromidis), Int. Conf. On Knowledge Discovery in Databases and Data Mining, KDD98, 1998, pp. 314-318.
69. Data Mining Approaches for Intrusion Detection, (with W. Lee), 1997 USENIX Security Conference, 1997.
70. JAM: Java Agents for Meta-Learning for Distributed Data Mining, (with A. Prodromidis, S. Tselepsis, W. Lee, W. Fan and P. Chan), Int. Conf. On Knowledge Discovery in Databases and Data Mining KDD97, (Runner Up Best Paper Award KDD-97), (short version accepted to AAAI97 Workshop).
71. Sharing Learned Models Among Remote Database Partitions by Local Meta-Learning, (with P. Chan), Int. Conf. On Knowledge Discovery in Databases and Data Mining, KDD96, Portland, Or., 1996.
72. Scaling Learning by Meta-Learning Over Disjoint and Partially Replicated Data, (with P. Chan), Florida AI Research Symposium, FLAIRS-96, Key West, Fl., 1996.
73. Learning Arbiter and Combiner Trees From Partitioned Data for Scaling Machine Learning, Int. Conf. on Knowledge Discovery in Databases and Data Mining, KDD95, Montreal, August 1995, pp. 39-44.
74. A Comparative Evaluation of Voting and Meta-learning on Partitioned Data, (with P. Chan), Proc. Int. Conf on Machine Learning 1995, ICML-95, Lake Tahoe, CA, pp. 90-98.
75. The Merge/Purge Problem for Large Databases, (with M. Hernandez), Proc. 1995 Intern. Conf. on Management of Data, SIGMOD-95, San Jose, CA, May 1995, pp. 127-138..
76. A Coding Approach to Event Correlation, (with S. Kliger, S. Yemini, Y. Yemini, D. Ohsie), Proc. Fourth IFIP/IEEE International Symposium on Integrated Network Management, 1995.
77. Predictive Dynamic Load Balancing of Parallel Hash-Joins over Heterogeneous Processors in the Presence of Data Skew, (with H. Dewan,K. Mok, and M. Hernandez), Proc. Intern. Conf. on Parallel and Distributed Information Systems, PDIS, Auston, TX, Sept. 1994, pp. 40-50.
78. Predictive Dynamic Load Balancing of Parallel and Distributed Rule and Query Processing, (with H. Dewan, M. Hernandez, and J. Wong), Proc. 1994 Intern. Conf. on Management of Data, SIGMOD-94, Minneapolis, MN, May, 1994, pp. 277-288..
79. Performance of Incremental Update in Database Rule Processing, (with D. Ohsie, H. Dewan, S. DaSilva), Proc. Research Issues in Data Engineering, RIDE-ADS, Houston, Texas, Feb. 1994, pp. 10-18.
80. Meta-level Control of Rule Execution in a Parallel and Distributed Expert Database System, (with. H. Dewan), Proc. Research Issues in Data Engineering, RIDE-ADS, Houston, Texas, Feb. 1994, pp. 105-114.
81. Experiments on Multi-strategy Learning by Meta-learning, (with P. Chan), Proc. Second Int. Conf. on Information and Knowledge Management, CIKM, Virginia, November 1993, pp. 314-323.
82. Dynamic Neighborhood Bounding in Monte Carlo Simulation, (with J. Glazier), Proc. 1993 Winter Simulation Conference, WSC, Dec. 1993.
83. Toward Multi-Strategy Parallel Learning in Sequence Analysis, (with P. Chan), First International Conference on Intelligent Systems for Molecular Biology, Washington, D.C., July, 1993, pp. 65-73.

84. Toward Parallel and Distributed Learning by Meta-learning, (with P. Chan), AAAI-93 Workshop on Knowledge Discovery in Databases (Precursor to KDD conference), 1993, pp. 227-240.
85. System Reorganization and Load Balancing of Parallel Database Rule Processing, (with H. Dewan), Proc. Seventh International Symposium on Methodologies for Intelligent Systems, Norway, June 1993, pp. 186-197, (published as chapter in book form).
86. A Parallel and Distributed Environment for Database Rule Processing, Open Problems and Future Directions, (with H. Dewan, D. Ohsie, M. Hernandez), AAAI Spring Symposium on Massive Parallelism in AI, Spring, 1993, pp. 207-215.
87. Is Production System Matching Interesting, (with M. Perlin, J. Carbonell, D. Miranker and M. Tambe), Proc. Tools for AI Conference, Washington, D.C., November, 1992, pp. 2-3.
88. The PARULEL Parallel Rule Language, (with H. Dewan and O. Wolfson), Proceedings Int. Conference on Parallel Processing, ICPP, Illinois, August 1991.
89. The ALEXSYS Mortgage Pool Allocation System,(with P. Chan, L. Woodbury, J. Glazier and D. Ohsie), Proc. IEEE Conference AI on Wall Street, New York, September, 1991.
90. Incremental Evaluation of Rules and its Relationship to Parallelism, (with O. Wolfson and H. Dewan), Proc. Intern. Conf. on Management of Data, SIGMOD-91, Denver, Colorado, May 1991.
91. The Constraint-Based Programming Paradigm, (with M. vanBiema and G. Maguire), Proceedings Hawaii Conference on System Sciences, January 1990.
92. Let's Stop the Dust from Collecting on OPS5, Proc. IFIP WG10.1 Concepts and Characteristics of Knowledge-based Systems), Nov. 1987, Mt. Fuji, Japan. appearing in Concepts and Characteristics of Knowledge-based Systems, North-Holland, 1989.
93. The Design and Implementation of a System Level Language for the DADO Parallel Machine, (with M. van Biema, M. Maguire, and G. Lerner), Proc. Twentieth Hawaii International Conference on System Sciences, Vol. 2, pp 152-162, January 1987.
94. The Do-Loop Considered Harmful in Production System Programming (with M. van Biema and D. Miranker), Proc. International Conference on Expert Database Systems, 1986.
95. The Application of AI and DADO Parallel Processor Technology to Future Unmanned Vehicle Systems, (with S. Alterman), (invited article), Proc. Symposium on Unmanned Vehicles, Johns Hopkins University, 1985, (selected for republication in Unmanned Systems, The Magazine of the Association for Unmanned Vehicle Systems, Vol. 4, No. 2, 1985, pp. 10-19).
96. A Simple Preprocessing Scheme to Extract and Balance Implicit Parallelism in the Concurrent Match of Production Rules (with D. Miranker and R. Mills), (invited article), Proc. Intern. Conf. on Fifth Generation Computer Architectures, IFIP, Manchester, England, 1985, pp. 1-10, (republished by North-Holland, 1986).
97. More Rules May Mean Faster Parallel Execution (with D. Miranker and R. Mills), (invited), Proc. AI and Distributed Problem Solving, Navy Research Laboratories, (sponsored by Office of Naval Research and National Academy of Sciences), 1985, National Academy Press, pp. 101-108.
98. Towards the Parallel Execution of Rules in Production System Programs (with T. Ishida), Proc. 1985 International Conference on Parallel Processing, ICPP, 1985, IEEE, pp. 568-575.
99. Are Maintenance Expert Systems Practical Now? (with P. Waldes and J. Lustgarten), (invited article), Proc. National Bureau of Standards Mechanical Failures Prevention Group Meeting on Artificial Intelligence, (to appear 1986 as an NBS publication).
100. An Overview of the DADO Parallel Computer (with M. Lerner and G. Maguire), (invited article), Proc. 1985 National Computer Conference, Chicago, IL, 1985, pp. 297-306.
101. On the Design of Parallel Production System Machines: What's in a LIP?, Proc. Hawaii International Conference on System Sciences, Hawaii, Vol. 1, 1985, pp. 232-237.
102. The Application of Artificial Intelligence Technology for Managing the Local Telephone Network (with G. Vesonder, J. Zielinski, F. Miller, and J. Wright), Proc. International Conference on Computer Communication, Australia, 1984.
103. Five Parallel Algorithms for Production System Execution on the DADO Machine, Proc. National Conference on Artificial Intelligence, Vol. 1, 1984, AAAI, pp. 300-307.
104. LPS Algorithms (with S. Taylor and A. Lowry), Proc. International Conference on Fifth Generation Computer Systems, Tokyo, Japan, 1984, ICOT, pp. 436-448.
105. Is CAD/CAM Ready for AI?, (invited paper), Proc. American Society of Mechanical Engineers, Computer Technology and CAD/CAM Meeting, San Antonio, TX, 1984, (selected for republication in the Journal of Applied Finite Elements and CAD/CAM).
106. DADO: A Parallel Processor for Expert Systems (with D. Miranker), Proc. 1984 International Conference on Parallel Processing, ICPP, MI, 1984, IEEE, pp. 74-82, (selected for republication in Computers for Artificial Intelligence Applications).

107. Logic Programming Using Parallel Associative Operations (with S. Taylor, A. Lowry, G. Maguire), Proc. IEEE International Symposium on Logic Programming, 1984, IEEE, pp. 58-69.
108. PROLOG on the DADO Machine: A Parallel System for High-Speed Logic Programming (with S. Taylor, C. Maio and D. Shaw), Proc. Phoenix Conference on Computers and Communications, 1984, IEEE.
109. Architecture and Applications of DADO: A Large-Scale Parallel Computer for Artificial Intelligence (with D. Miranker and D. Shaw), Proc. International Joint Conference on Artificial Intelligence, IJCAI, Karlsruhe, West Germany, Vol. 2, 1983, IJCAI, pp. 850-854.
110. ACE: An Expert System for Telephone Cable Maintenance, (with G. Vesonder, J. Zielinski, F. Miller and D. Copp), Proc. International Joint Conference on Artificial Intelligence, IJCAI, Karlsruhe, West Germany, Vol. 1, 1983, pp. 116-121.
111. Knowledge Engineering: Theory and Practice, Proc. IEEE Conference on Trends and Applications in Science, Washington DC, 1983, IEEE, pp. 97-104.
112. DADO: A Tree-Structured Machine Architecture for Production Systems (with D. Shaw), Proc. National Conference on Artificial Intelligence, Vol. 1, 1982, AAAI, pp. 242-246.
113. Automatic Discovery of Heuristics for Nondeterministic Programs, (with M. Harrison), Proceedings Sixth International Joint Conference on Artificial Intelligence, IJCAI 1979, pp. 853-856.

Workshop Papers Peer Reviewed

1. Fox in the Trap: Thwarting Masqueraders via Automated Decoy Document Deployment, Jonathan Voris, Jill Jermyn, Nathaniel Boggs and Salvatore Stolfo, ACM European Workshop on System Security, 2015.
2. Model Aggregation for Distributed Content Anomaly Detection, Sean Whalen, Nathaniel Boggs and Sal Stolfo, AI Security Workshop, CCS, 2014.
3. On the Use of Decoy Applications for Continuous Authentication on Mobile Devices, Malek Ben Salem, Jon Voris and Salvatore Stolfo, Who are you?! Adventures in Authentication: WAY Workshop (WAY) 2014.
4. System level user behavior biometrics using Fisher features and Gaussian mixture models, (w. Y. Song, M. Ben Salem and S. Hershkop), Workshop on Research in Insider Threat (WRIT), 2013.
5. "The MEERKATS Cloud Security Architecture", (with Angelos D. Keromytis, Roxana Geambasu, Simha Sethumadhavan, Salvatore J. Stolfo, Junfeng Yang, Azzedine Benameur, Marc Dacier, Matthew Elder, Darrell Kienzle, and Angelos Stavrou), In Proceedings of the 3rd International Workshop on Security and Privacy in Cloud Computing (ICDCS-SPCC), pp. 446 - 450. June 2012, Macao, China.
6. Fog Computing: Mitigating Insider Data Theft Attacks in the Cloud. Salvatore J Stolfo, Malek Ben Salem and Angelos Keromytis, Workshop on Research on Insider Threats, WRIT, 2012.
7. Lost in Translation: Improving Decoy Documents via Automated Translation, Jonathan Voris, Nathaniel Boggs and Salvatore Stolfo, Workshop on Research on Insider Threats, WRIT, 2012.
8. Concurrency Attacks, (with Junfeng Yang, Ang Cui, Sal Stolfo and Simha Sethumadhavan), Proceedings USENIX Workshop on Hot Topics in Parallelism (HotPar), 2012.
9. ALDR: A New Metric for Measuring Effective Layering of Defenses, (with N. Boggs), ACM CCS Layered Assurance Workshop (LAW), 2011.
10. On the Design and Execution of Cyber-security User Studies: Methodology, Challenges, and Lessons Learned, (with M. Ben Salem), Proc. 4th Workshop on Cyber Security Experimentation and Test (CSET '11), 2011.
11. Killing the Myth of Cisco IOS Diversity: Towards Reliable, Large-Scale Exploitation of Cisco IOS, (with A. Cui and J. Kataria), USENIX Security Workshop on Offensive Technologies (WOOT '11), 2011. (Talk presented at Black Hat 2011)
12. "The MINESTRONE Architecture: Combining Static and Dynamic Analysis Techniques for Software Security" (with Angelos D. Keromytis, Salvatore J. Stolfo, Junfeng Yang, Angelos Stavrou, Anup Ghosh, Dawson Engler, Marc Dacier, Matthew Elder, and Darrell Kienzle), In Proceedings of the 1st Workshop on Systems Security (SysSec). July 2011, Amsterdam, Netherlands.
13. "The SPARCHS Project: Hardware Support for Software Security", (with Simha Sethumadhavan, Salvatore J. Stolfo, David August, Angelos D. Keromytis, and Junfeng Yang), In Proceedings of the 1st Workshop on Systems Security (SysSec). July 2011, Amsterdam, Netherlands.
14. Reflections on the Engineering and Operation of a Large-scale Embedded Device Vulnerability Scanner, (with A. Cui), Building Analysis Datasets and Gathering Experience Returns for Security, (BADGERS), April, 2011.
15. Detecting Masqueraders: A Comparison of One-Class Bag-of-Words User Behavior Modeling Techniques", Malek Ben Salem and Salvatore J. Stolfo, Insider Threat Workshop MIST 2010. (Best Paper Award)

16. Keep Your Friends Close: The Necessity for Updating an Anomaly Sensor with Legitimate Environment Changes, (with G. Cretu-Ciocarlie, A. Stavrou, M. Locasto), ACM Computer and Communications Security Conf. Workshop AI in Security, AISEC, 2009.
17. Return Value Predictability Profiles for Self—Healing, (with M. E. Locasto, A. Stavrou, G. F. Cretu, A. D. Keromytis), Third International Workshop on Security (IWSEC 2008), 2008.
18. Automated Social Hierarchy Detection through Email Network Analysis, (with R. Rowe, G. Creamer and S. Hershkop), in Proceedings of the Web Mining and Social Network Analysis Workshop on International Conference on Knowledge Discovery and Data Mining (KDD), San José, CA, 2007.
19. Fileprints: Identifying File Types by n-gram Analysis, (with W. Li, K. Wang, and Benjamin Herzog), 6th IEEE Information Assurance Workshop, May 2005.
20. Towards Collaborative Security and P2P Intrusion Detection**,** (with M. E. Locasto, J. J. Parekh, and A D. Keromytis), 6th IEEE Information Assurance Workshop, May 2005.
21. Email Archive Analysis Through Graphical Visualization, (with W. Fei, and S. Hershkop), Proceedings of the 2004 ACM Workshop on Visualization and Data Mining for Computer Security (VizSEC/DMSEC-2004), ICDM, 2004.
22. One-Class Training for Masquerade Detection, (with K. Wang), 3rd IEEE International Conference on Data Mining, Workshop on Data Mining for Security Applications, Florida, Nov., 2003.
23. One Class Support Vector Machines for Detecting Anomalous Window Registry Accesses, (with K. Heller, K. Svore, A. Keromytis), 3rd IEEE International Conference on Data Mining, Workshop on Data Mining for Security Applications, Florida, Nov., 2003.
24. A Holistic Approach to Service Survivability, (with A. Keromytis, J. Parehk, P. Gross), ACM Workshop on Survivable and Self-Regenerative Systems, Sept. 2003.
25. A Behavior-based Approach to Security Email Systems, (with S. Hershkop, K. Wang, O. Nimeskern, and C. Wu), Intl. Workshop on Mathematical Methods, Models and Architectures for Computer Networks Security, September 20-24, 2003, St. Petersburg, Russia.
26. MET: An Experimental System for Malicious Email Tracking, ACM New Security Paradigms Workshop, Virginia Beach, VA, Sep, 2002.
27. Intrusion Detection with Unlabelled Data using Clustering, (with L. Portnoy, and E. Eskin), ACM Computer Communication Security Workshop on Data Mining for IDS, Nov. 2001.
28. Toward Cost-Sensitive Modeling for Intrusion Detection and Response, (with W. Lee, W. Fan, M. Miller, and E. Zadok), Workshop on Intrusion Detection and Prevention, 7th ACM Conference on Computer Security, Athens GR, November, 2000.
29. Adaptive Model Generation for Intrusion Detection, (with E. Eskin, M. Miller, Z. Zhang, G. Yi, L. Wei-Ang), Proc. ACM CCS Workshop on Intrusion Detection and Prevention, 2000.
30. Cost complexity-based pruning of ensemble classifiers (with A. Prodromidis), ACM SIGKDD Workshop on Distributed and Parallel Knowledge Discovery, 2000.
31. Towards Automatic Intrusion Detection Using NFR, (with W. Lee and C. Park), In the 1st USENIX Workshop on Intrusion Detection and Network Monitoring, 1999.
32. Using conflicts among multiple base classifiers to measure the performance of stacking, (with W. Fan, and P. Chan), Working Notes ICML-99 Workshop on Recent Advances in Meta-Learning, 1999.
33. The Effects of Training Class Distribution on Performance Using Cost Models, (with Phillip Chan), KDD98 Workshop on Distributed Data Mining, 1998.
34. Pruning Classifiers in a Distributed Meta-Learning System, (with A. Prodromidis and P. K. Chan), KDD98 Workshop on Distributed Data Mining, 1998.
35. Data Mining over Distributed Databases and its Application to Fraud and Intrusion Detection in Financial Information Systems, NSF Workshop on R&D Opportunities in Federal Information Services, May 1997.
36. OS-level Intrusion Detection using Meta-Learning Agents, AAAI 97 Workshop on AI Approaches to Fraud Detection and Risk Management, 1997.
37. Credit Card Fraud Detection Using Meta-Learning: Issues and Initial Results with (D. Fan, W. Lee, A. Prodromidis and P. Chan), AAAI 97 Workshop on AI Approaches to Fraud Detection and Risk Management, 1997.
38. JAM: Java Agents for Meta-Learning for Distributed Data Mining, (with A. Prodromidis, S. Tselepsis, W. Lee, W. Fan and P. Chan), AAAI 97 Workshop on AI Approaches to Fraud Detection and Risk Management, 1997.
39. A Comparative Evaluation of Combiner and Stacked Generalizations, (With D. Fan and P. Chan), AAAI-96 Workshop on Integrating Multiple Learned Models, IMLM-96, Portland, Or., 1996.
40. Integrating Multiple Learned Models for Improving and Scaling Machine Learning Algorithms, AAAI96 Workshop, Working Notes, August, 1996.

41. Scalable Active Databases, Schloss Dagstuhl Seminar Report, 1994.
42. Meta-Learning for Multi-Strategy and Parallel Learning, (with P. Chan), Second International Workshop on Multi Strategy Learning, 1993, pp. 150-165.
43. Parallel Programming of Rule-based Systems in PARULEL, (with M. Hernandez), IJCAI Work. on Parallel Production Systems, International Joint Conference on AI, France, August, 1993, pp. 3-12.
44. Knowledge Discovery in Very Large Databases by Parallel Meta-learning, First DARPA Workshop on Intelligent Information Integration Systems, Reston, VA, March 1993, pp. 39-40.
45. The ALEXSYS Mortgage Pool Allocation Expert System: A Case Study of Speeding up Rule-based Programs, (with L. Woodbury, J. Glazier and P. Chan), Proc. AI and Business Workshop Proceedings, American Association of Artificial Intelligence, Boston, August, 1989.
46. Speech Recognition in Parallel, (with Z. Galil, K. Mckeown, and R. Mills), Proc. DARPA Speech and Natural Language Workshop, Cape Cod, Mass., October 1989.

Other publications

1. Does profiling make us more secure? Pfleeger, S.L., Rogers, M., Bashir, M., Caine, K., Caputo, D., Losavio, M., Stolfo, S. 2012, IEEE Security and Privacy 10 (4) , art. no. 6265096 , pp. 10-15

Technical Reports

1. "Smashing the Stack with Hydra: The Many Heads of Advanced Polymorphic Shellcode", Pratap V. Prabhu Yingbo Song and Salvatore J. Stolfo, 2010.
2. Automatically Parallelizing Legacy Binary Code for MultiCore Architectures, (with D. August, M. Locasto and S. Sethumadhavan), AFRL-RY-WP-TR-2009, DARPA Seedling final report, August 2009.
3. BARTER: A Model Exchange Access Control and Communication Framework for Secure Content Mobile Ad-hoc Networks, (with V. Frias-Martinez), CU Tech Report,
4. Quantifying Application Behavior Space for Detection and Self-Healing, (with M. Locasto, A. Stavrou, G. Cretu and A. Keromytis), CU Tech Report 017-06,
5. Privacy-Preserving Paylod-Based Correlation for Accurate Malicious Traffic Detection, (with. J. Parekh, and K. Wang), CU Tech Report 026-06, May 2006
6. Host-based Anomaly Detection Using Wrapping File Systems, Shlomo Hershkop, Ryan Ferster, Linh H. Bui, Ke Wang and Salvatore J. Stolfo. *CU Tech Report* April 2004.
7. Collaborative Distributive Intrusion Detection, Michael E. Locasto, Janak J. Parekh, Salvatore J. Stolfo, Angelos D. Keromytis, Tal Malkin, Vishal Misra. *CU Tech Report CUCS-012-04*, 2004.
8. EMT/MET: Systems for Modeling and Detection of Errant Email, DARPA DISCEX III, April 2003.
9. Database Research at Columbia University, (with S. Chang, L. Gravano, G. Kaiser, K. Ross), SIGMOD Record, Vol 27, No. 3, September 1998, 75-80.
10. Approximate String Matching on the DADO Parallel Computer, (with T. Mori), Department of Computer Science Technical Report, Columbia University, 1988.
11. A Note on Implementing OPS5 Production Systems on DADO, Department of Computer Science Technical Report, Columbia University, 1984.
12. ||PSL: A Parallel Lisp for the DADO Machine (with M. van Biema, M. Lerner, and G. Maguire), Department of Computer Science Technical Report, Columbia University, 1984.
13. Research Issues in the Development of Expert Systems, (with G. Vesonder, F. Miller, J. Zielinski, and D. Copp), Bell Labs Technical Memorandum, May, 1983.

Technical Presentations

1. RSA 2015, Hot Research Topics: Symbiote Technology, Decoy Technology, April 2015.
2. Office of the Secretary of the Air Force, Embedded Insecurity, January 2015.
3. AFEI Conference, CyberWest, DHS invitational talk on Symbiote technology.
4. DHS Embedded System Insecurity, Mar 2013.
5. DoD OSD (Pentagon), Cisco IP Phone vulnerabilities, February 2013
6. DHS Briefing, Cisco IP Phone vulnerabilities, January 2013
7. IARPA Briefing, Cisco IP Phone vulnerabilities, January 2013
8. Amphion Forum, Cisco IP Phone vulnerabilities, San Francisco, Dec 2012.
9. Embedded Systems Security, RSA Panel, 2012
10. Embedded Insecurity, Symantec, Feb 2012

11. Killing the Myth of Cisco IOS Diversity, Black Hat 2011
12. Security Metrics, Defense Science Board, March 2011
13. Quantitative Analysis of a wide area scan for vulnerable devices, DHS ITTC meeting, SRI, Feb 2011
14. Polymorhpic Shellcode: The Demise of Signature-based Detection

` 1 Sandia National Labs, March 2010.
2 Invitation, U Cal Berkeley, Nov, 2009.
3 Invitation MIT LL, June 2009.
4 Invitation ORNL, June 2009.

15. Network Analytics, C3E Workshop, Invitation, Santa Fe, July 2009
16. Advanced research in IDS, MITRE, June 2009..
17. Insider Attack Detection, InfoSec, ACNS, CA, 2008.
18. I3P Insider Attack Project Review, 2007.
19. Payload-based Anomaly Detection, IBM/CU/Stevens Security Day, 2007.
20. Insider Threat research I3P Meeting, GA Tech, , December 2006.
21. DNI/DTO Invitation only Workshop, New Research on Privacy-preserving data mining, December 2006.
22. DARPA ISAT Meeting on Advanced Machine Learning Research, August 2006.
23. DARPA Advanced IDS Meeting, Overview of research on advanced IDS, Feb 2007.
24. DNI/DTO PI Meeting, Large-Scale System Defense, March 2007.
25. ARO PI meeting, Masquerader Detection. August 2006
26. Invited talk, Collaborative Security, Global Security Consortium, Washington, DC, Oct 2005.
27. Invited talk, Advanced Stealthy Malware attacks, ARO Malware Workshop, Washington, DC, August 2005.
28. Invited talks on "Behavior-based Computer Security" (2003-2005),
29. Adversarial Learning in Computer Security, NIPS Workshop, 2007.
    1. ISMIS 2005, Saratoga Springs, NY, Keynote talk.
    2. Federal Aviation Administration,
    3. DARPA IRC Meeting, Hard Technical Problems,
    4. IEEE ICDM-2003, Int. Workshop on Data Mining for Security Applications
    5. Griffiss Institute Conference, November, 2003,
    6. International Workshop on Mathematical Methods, Models and Architectures for Computer Networks Security", St. Petersburg, Russia, September 2003,
    7. Government Convention on Emerging Technologies, Defending America Together: The New Era, Las Vegas, Jan, 2003,
    8. NIST ACIT Workshop on Insider Threat, Feb 2003,
    9. Griffiss Institute Meeting on Information Assurance and Cyber Security, Utica, Feb 2003,
    10. Polytechnic University, May 2003,
    11. Workshop on Machine Learning in Computer Intrusion Detection, GMU, Sept 2003.
30. Invited talks and briefings on Data Mining Based Intrusion Detection, 2002-2003,
    1. EDS, Lockheed Martin, CACI, White House, DoD (PACOM, AFCERT), NSA, CIA, OSD, DISA, CISCO, Symantec
31. Invited State of the Field Talk, Data Mining, Supercomputing 2000.
32. Invited lecture, The JAM Project and Intrusion Detection, IBM Yorktown Heights, May, 1999.
33. Invited participant, White House/DOE Invitational Workshop on Detection of Malicious code, Intrusions, and Anomalous Activity Workshop, Washington, February, 1999.
34. Keynote Speaker, Advance Information Technologies for Government Conference, Washington D.C., September, 1998.
35. Panelist, KDD98, Distributed Data Mining Workshop, August, 1998.
36. Invited Lecture, The JAM Project, Java Agents for Meta-Learning
    1. NISS Workshop on Security and Privacy of Statistical Information, Washington, D.C., September, 1997
    2. Classification Society of North America Conference, CSNA-97, June 1996.
37. Fraud and Intrusion Detection
    1. Panelist, Computer Misuse and Anomaly Detection Workshop, Monterey CA, November 1996
    2. Panelist, SPIE 1996, Boston, November 1996
    3. DARPA ITO IDS meeting, Rome Labs, Boston, November 1996
    4. DARPA ITO IDS meeting, Santa Cruz, CA, September 1996
38. Invited Lecture, Parallel and Distributed Database Inference and Applications, MIT AI Lab, February, 1996
39. Parallel and Distributed Database Inference and Applications, IBM, Hawthorne, NY, December 18, 1995
40. Merge/Purge for Large Data Bases

    1. Polytechnic University CATT, Corporate Research Review, December 12, 1995
    2. Citicorp, CTO, October 1995.
41. Scalable Data Mining, NYU Stern Business School, November, 1995.
42. Learning Arbiter and Combiner Trees From Partitioned Data, First Int. Conf. on Knowledge Discovery in Databases, August 1995, Montreal, Canada.
43. Parallel and Distributed Database Inference, Polytechnic University CATT Forum, March, 1995.
44. Scalable Active Databases, Schloss Dagstuhl, Internationales Begegnungs-Und Forschungszentrum Fur Informatik, March 1994.
45. Parallel Production System Languages, Workshop on Innovative Applications of Production Systems, IJCAI Conference, Chambery, France, August 1993.
46. Parallel processing of Merge/Purge, Axciom Corporation, March 1993.
47. Scalable Machine Learning by Meta-learning, First DARPA Workshop on Intelligent Information Integration Systems, March, 1993.
48. Integrating Large Data and Knowledge Bases, NSF Workshop on HPCC and AI, February 1992.
49. Is Production System Matching Interesting, Panel Discussion and Presentation, Tools for AI Conference, Washington, D.C., November, 1992, pp. 2-3.
50. The PARULEL Parallel Rule Language, International Conference on Parallel Processing, Illinois, August 1991.
51. Research At Columbia's Center for Advanced Technology, Long Island Forum for Technology, 1990.
52. Speech Recognition in Parallel
    1. Univ. of Connecticut, November 1989.
    2. DARPA workshop on Speech and Natural Language Processing, October 1989.
53. Testimony on FCCSET and SIAM reports on the National Supercomputing Initiative, Office of Science and Technology Policy, Rayburn Building, Washington D.C., February, 1988.
54. Let's Stop the Dust from Collecting on OPS5, IFIP WG10.1 Workshop on Concepts and Characteristics of Knowledge-based systems, Mt. Fuji, Japan, November 1988.
55. On the Limitations of (SIMD) Massively Parallel Computers for Logic Programming, First NSF/ICOT Workshop on Artificial Intelligence, November 1988.
56. The DADO Machine and its Application, MIT Lincoln Laboratories, November 1986, RCA Laboratories, NJ, May, 1985, Asilomar Microcomputer Workshop, Monterey, CA, 1985, MCC, Austin TX, November, 1984
57. Five Parallel Algorithms for Production Systems, New York University, Ultra-computer Project seminar, 1985.
58. Parallelism in New Generation Computing, invited panelist, 1984 International Conference on Fifth Generation Computing, Tokyo, Japan, November, 1984.
59. Expert Systems and AI, Long Island ACM Chapter Meeting, NY, May 1984.
60. Knowledge Engineering: Theory and Practice
    1. National Defense Science Board, December 1983
    2. LIFT Business Organization, October 1983
    3. Intel Corporation, October 1983
    4. Honeywell Corporation, October 1983
    5. Naval Research Laboratory, September 1983
    6. ONR Contractor's Meeting, September 1983, Carnegie-Mellon University, September 1983
    7. IBM/Columbia Technical Symposium, White Plains, NY, March 8, 1983
61. NON-VON and DADO: Two Parallel Architectures, Seminar in AI, Rutgers University, NJ, April 15, 1983.
62. AI Research at Columbia University, Brooklyn College, City University of New York, NY, March 5, 1983.
63. Expert Systems
    1. AIL Division, Eaton Corporation, NY, March 4, 1983,
    2. Grumman Corporation, NY, 1982,
    3. Office of Naval Research/National Bureau of Standards Workshop on Automated Manufacturing Research, Gaithersburg, MD, 1982.
64. An Overview of the DADO Project
    1. IBM/Columbia Technical Symposium, White Plains, NY, March 7, 1983
    2. Digital Equipment Corporation, MA, February 25, 1983
    3. Workshop on Parallel Architectures, Sponsored by Lawrence Livermore Laboratories, Boulder, CO, January 20, 1983
    4. Parallel Processing Workshop, New York University, NY, April 1982

65. Advanced Architectures, Invitational panel session at the Third International Conference on Distributed Computing Systems, Miami, FL, October 20, 1982.

Research Contracts and Grants

(Total for which I have records since 1982: over $49,500,000, average over $1,200K/year)

1 DARPA Active Authentication, Phase 2, Active Authentication: Search Behavior and Decoy Technology, Allure Security Technology, Inc., $2.1 M, 2013-2015.
2 DARPA VET, Red Balloon Security(A Columbia spinout), Automatic Firmware Analysis as a Cloud Service, $4.3Mil, 2013-2015
3 DARPA SBIR, Automatic Repair of Vulnerable Firmware, Red Balloon Security, $100K, 2013.
4 DARPA Cyber Fast Track, SBIR, Red Balloon Security, (A Columbia spinout), $273K, 2013.
5 DARPA Cyber Fast Track, SBIR, Red Balloon Security, (A Columbia spinout), $150K, 2012.
6 DHS Advanced Situation Awareness of High Impact Attacks against the routing infrastructure, $720K, 2012-2013.
7 DARPA CRASH, incremental funding for research staff, (joint with Simha), $450K, 2012-2013.
8 AFOSR Designing for Measurable Security, $1,890K, 2011-2017
9 DARPA MRC, MEERKATS Project, $6,500K, 2011-2014.
10 DARPA Active Authentication Program, Allure Security Technology (A Columbia spinout), $500K, 2012.
11 DARPA SBIR, Allure Security Technology (A Columbia spinout), Phase 2, $1,500K, 2011.
12 DARPA SBIR, Allure Security Technology (A Columbia spinout), Phase 1, $150K, 2011.
13 DARPA ADAMS – Advanced Behavioral Sensors, (w/ A. Keromytis) $780K, 2011-2013.
14 DARPA CRASH/SPARCHS, joint with several faculty and Princeton, $6.4M, 2010-2013.
15 IARPA STONESOUP Program, MINESTRONE, joint with several faculty, $500K, 2010-2013.
16 NSF EAGER, Measuring the Security Posture of Large Financial Organizations, the Human Factor, NSF, $300K, 2009.
17 AFOSR DURIP Equipment Grant, $650K, 2009.
18 Botnet Threat, ONR Joint with Yale, $295K, 2009.
19 DHS S&T, Privatized Network Traces (joint with BAE), 2008-2009, Phase 1: $500K, Total $2,000,000.
20 Symantec Gift, $32.5K, 2009.
21 IARPA, Secure Private Querying, $600K (shared by 4 PI's), 2008.
22 DARPA National CyberRange, Phase 1, (joint with BAE), 2009, $70K.
23 DARPA, Automatically Parallelizing Legacy Binary Code for Multi-Core Architectures *via* Extraction of Self-Similarity, $85K, June 2008-May 2009.
24 ARO/NSA, Distributed Network Anomaly Detection and Insider Threats, $412K, Jan 2006 – Dec 2009.
25 NSF CyberTrust, CT-T: Enabling Collaborative Self-healing Software systems, $808K, Sept 2006 – Aug 2009.
26 AFRL MURI joint with GMU, $1.3 million over 5 years.
27 DHS/I3P Insider Threat Project, $600K over 18 months, 2007-2008.
28 Google research grant, 2007 $25K, 2008 25K.
29 NYSTAR CAT, Social Network and Document Flow Analysis, NYSTAR CAT, $20K, Jun – Dec 2006.
30 DTO (NSA, formerly ARDA), Large-Scale System Defense, DTO, $500K, 18 months.
31 DARPA, Model Exchange for Access Control in MANETS, $200K, 2006-2007.
32 NIST/ARO, BARTER: Model Exchange for Access Control and Security in Mobile Ad Hoc Networks, $25K, Jan 2006 – Dec 2006.
33 NSA, Phase 2 Distributed Network Anomaly Detection, $200K, Jan 2006 – Dec 2006.
34 ARDA Malware Challenge Problem, Detecting Data-driven malware, $74K, Jan 2006-Aug 2006.
35 ARO, Insider Attack Detection, $200K, Jan 2007 – Dec 2008.
36 ARO Grant, Stealth and Counter-Evasion Techniques, $50K, Oct 2005 – Sept 2006.
37 NSF DG Email Mining for Supporting Forensics for Law Enforcement, Sep 2005-Sep 2006, $100K.
38 Collaborative Security, DHS/ARO, $136K, October 2004-October 2005.
39 DHS SBIR Grant, Cross Domain Collaborative Security, DHS, $33K, Oct 2004-Oct 2005.
40 DHS SBIR Grant, Malicious Code Detection, DHS, $33K, Oct 2004-Oct 2005.
41 ARDA/PNL, Malware Challenge Problem, $10K, May 2005.
42 NSF Workshop on Resilient Financial Information Systems, $25K, May 2005 – April 2006.
43 NSF DG Email Mining for Supporting Forensics for Law Enforcement, Sep 2004-Sep 2005, $100K.
44 Maryland Procurement Office, Dept. of Interior, Distributed Intrusion Detection Feasibility Study, $300K, April 2003 – March 2004.

45 DARPA Cyber Panel Grant, Application Level IDS, $300,000, Sept 2002-Sept 2003.
46 In-Q-Tel, Email Mining Toolkit, $74,000, Jan 2003.
47 NSF SGER joint with Columbia Business School, $100,000, 2001-2002.
48 DARPA Grant with NFR, Incremental Update of IDS, $200,000, 2001-2002.
49 ITT Grant for research on Correlation in Intrusion Detection Systems, $100,000, 2000.
50 DARPA Grant, Cost-sensitive Modeling for Intrusion Detection, joint with NCSU and FIT, $900,000, 3 years, 2000-2002.
51 DARPA STTR Grant, Phase I, with NFR Corporation, $35,000, 2000.
52 DARPA STTR Grant, Phase I, with RST Corporation, $38,000, 2000.
53 NSF Digital Government Program, The CARDGIS Energy Data Collection, joint with USC/ISI, $1,500,000 for 3 years.
54 NSF CISE Infrastructure Grant to Department of Computer Science, $42,000 in first year, 1996-2000.
55 Scalable Data Mining by Meta-Learning, NSF Data Base and Expert Systems and Knowledge and Cognitive Modeling Programs, $153,000 for 3 years, Starting July 1996.
56 Fraud and Intrusion Detection for Financial Information Systems, ARPA Grant, BAA96-03, Survivable Information Systems, joint with FIT, $1,000,028 for 3 years, 1996-1999.
57 Scalable Data Mining by Meta-Learning Agents, Polytechnic University CATT, $60,000, July 1996- June 1997.
58 Parallel and Distributed Intelligent Systems, Polytechnic University CATT, $55,000, 1995-1996.
59 Scalable Parallel and Distributed Expert Database Systems, NSF, $80,000, IRI 93-13847, 1994-1995.
60 Scalable Parallel and Distributed Pattern-directed Inference Systems for Fraud Detection, Polytechnic University CATT, $55,000, July 1, 1994-June 30, 1995.
61 Citicorp CTO, Parallel Database Inference Processing, $25,200 PhD Stipend, 1993 - 1994, $43,200 1994-1995.
62 GTE Labs, $14,000 for GRA stipend (Philip Chan), Summer 1992.
63 D.E. Shaw & Co., $5,000, Donation to CS/CAT Industrial Affiliates, 1992.
64 Citicorp CTO, $36,000 for network services and consulting, 1992, 1993, 1994, 1995.
65 Donation of DEC station 5000, Digital Equipment Corporation, October 1990, $99,600.
66 Citicorp NAIB support for joint expert system research project through Columbia Center for Advanced Technology 1989, $50,000.
67 Donation in support of DADO4 development, static memory chips, IDT Corporation, 1989, $30,000.
68 Defense Advanced Research Projects Agency, Research in Parallel Processing, November 1987-June 1989, $554,000.
69 Defense Advanced Research Projects Agency, Strategic Computing Program support for the DADO Project. (1985: $560,000)
70 Valid Logic Systems, donation of 2 Computer Aided Engineering workstations. (1984: $180,000)
71 New York State Science and Technology Foundation, Massively Parallel Processing support as part of the Center of Advanced Technology in Computers and Information Systems. (1984: $181,000, 1985: $222,000, 1986: $220,000, 1987: $180,000, 1988: $180,000, 1989: 173,000, 1990: $200,000, 1991: $185,000, 1992: $180,000, 1993: $180,000).
72 Fifth Generation Licensing Payments for support of Research, (1987: $44,000, 1986: $40,000, 1985: $14,000.).
73 AT&T Foundation, Research in Speech Generation (Nathaniel Polish), 1986: $25,000.
74 The DADO Project, Defense Advanced Research Projects Agency. (1984: $560,000)
75 Specialized Architectures for Production Systems, Defense Advanced Research Projects Agency. (1982-1983: $512,000)
76 Learning Problem Solving Strategies in Knowledge Engineering, Office of Naval Research, 1982-1985. (1982-1984: $240,000)
77 IBM Corporation, donation of hardware components for the DADO Project as well as stipend monies for two of my Ph.D. students. (1983-1984: $20,000)
78 Intel Corporation, donation of hardware and components for the DADO Project. (1982: $30,000)
79 IBM Faculty Development Award. (1984-1985: $60,000)
80 Hewlett-Packard Corporation, 8 Computer Workstations, (1984: $676,000).

Ph.D. Students

1. Daniel Miranker, completion October 1986: “Treat: A New and Efficient Match Algorithm for Production System”, Associate Professor with tenure University of Texas at Austin.
2. Stephen Taylor, left program in 1985 with MS to complete PhD at Technion, Professor at Dartmouth.

3. Alexander Pasik: “More Parallelism in Production Systems”, completion May, 1989, Vice President, Gartner Group.
4. Michael van Biema: “The Constraint-based Programming Paradigm”, completion November 1989, Associate Professor Columbia University.
5. Russell Mills: The llc Parallel Programming Language, Ph.D. awarded posthumously, 1992.
6. Nathaniel Polish: Knowledge-based Speech Generation, completed January, 1993, President NPS Associates.
7. Hasanat Dewan: Paradiser Project, Predictive Dynamic Load Balancing, completion May 1994, VP of R&D, Deutschebank.
8. Jason Glazier: Dynamic Neighborhood Variance Reduction for Monte Carlo Simulations, September 1994. Vice President Morgan Stanley.
9. David Espinosa: Semantic Lego: Formal specification of programming language interpreters, March 1995, Member Technical Staff of Kestrel Institute.
10. Mauricio Hernandez: The Merge/Purge Problem as a Generalization of Band Joins, March 1996, Assistant Professorship, University of Illinois, Springfield.
11. Philip Chan: Distributed and Parallel Meta-learning, October 1996, Associatet Professor, Florida Institute of Technology.
12. David Ohsie: Event Correlation in Network Management, May 1998, Member of Technical Staff, System Management Arts, Inc.
13. Andreas Prodomidis: Strategies for Combining Multiple Classifiers, May 1999, Director of R&D, Greek National Bank.
14. Wenke Lee: Data Mining Approaches to Intrusion Detection, May 1999, Asst. Professor Georgia Tech.
15. Wei Fan: Conflict resolution of multiple classifiers, December 2000, Member of Tech Staff IBM Research.
16. Eleazar Eskin, Sparse Sequence Analysis, Asst. Professor, UC San Diego, December 2002.
17. Shlomo Hershkop, Email Mining Toolkit, Asst. Professor, Columbia University, July 2005.
18. German Creamer, Applied Machine Learning to Financial Information, Expected June 2006
19. Ke Wang. Content-based Payload Anomaly Detection. August 2006, Google CA.
20. Janak Parekh (co-advised with Kaiser), February 2007, Google NY.
21. Wei-Jen Li, Insider Detection of Malware bearing documents. June 2008.
22. Vanessa Frias-Martinez, Behavior-based Access Control, October 2008.
23. Gabriella Cretu, Towards Fully Automated Anomaly Detection Sensors, September 2009.
24. Brian Bowen, Decoy Network Traffic, Dec 2010.
25. Malek Ben Salem, User command intent modeling for Masquerade Detection, Expected Dec 2010.
26. Yingbo Song, Generating Private Traces, January 2012.
27. Ang Cui, New, Expected 2015.
28. Nathaniel Boggs, Expected 2015.
29. David Tagatac, Expected 2016.
30. Adrian Tang, Expected 2016.
31. Yuan Kong, Expected 2075.

Master’s Students

Supervised dozens of Master’s Projects in Knowledge Engineering, Parallel Processing, Distributed Machine Learning.

University Service

- CS Department Retreat, Subgroup leader on Large-Scale Parallelism, 2008.
- Columbia College Core Curriculum Committee on Science Instruction, 2006-2007.
- Homeland Security committee with Provost Cole, Apr 2003.
- Chair, CS Faculty Recruiting Committee, 1997-1998.
- Organizer, Joint meeting with USC/ISI on the Digital Government Initiative, 1998.
- Academic Committee, 1995-1996.
- NSF CISE Infrastructure Grant Committee, 1996.

- Acting Chairman, Computer Science Department, Columbia University, November 1986 - June 1987. Duties include: Management of Departmental budget, including the successful resolution of a major financial deficit position. All department administrative matters. Faculty development and promotion cases.
- Director, Center for Advanced Technology in Computers and Information Systems, 1988 - 1990. Duties include: Management and responsibility for $2 million yearly budget.
- Regular meetings in Albany, Syracuse and Manhattan to perform duties. These include lobbying meetings called by the Foundation, and engagements with prospective industrial sponsors.
- Presented awards at the New York Academy of Sciences for the New York City finalists in the Westinghouse Young Scientists Competition.
- Evaluated several New York companies for the NYSSTF who applied for funding under various programs.
- Information Systems Subcommittee to the University Committee on Budget and Planning, 1990-1992, 1993-1994.
- Software Policy Committee, 1991.
- Chairman Search Committee, October 1986.
- Representative to GS Division Committee on Instruction.
- Liaison, New York City Partnership University/Industry Joint Pilot Project, 1989 - present.
- Speaker, numerous Computer Science Department sponsored meetings with industrial representatives of IBM, AT&T, Sperry, DEC, Aetna, Exxon, GE and GM.
- SEAS Faculty Contact Program.
- IBM Proposal Committee.
- Department Central Facilities Committee.
- Ph.D. Assignment Committee.
- DEC External Research Grant Proposal Committee.
- New York State Science and Technology Foundation Center for Advanced Technology Proposal Committee.
- Defense Advanced Research Project Agency Equipment Proposal Committee.
- Defense Advanced Research Projects Agency Proposal Committee.
- Chairman, Computer Science Department Colloquia Series.
- AI Ph.D. Qualifying Examination Committee.
- Computer Science Undergraduate Curriculum Committee.
- Barnard College Committee on Instruction.
- Liaison, Bell Labs One Year On Campus Program.
- Advisor, Barnard College Computer Science Majors.
- Advisor, Columbia College Computer Science Majors.
- Advisor, General Studies Computer Science Majors.
- Advisor, Computer Science Master's students.

Teaching Evaluations at Columbia

Consistently excellent student evaluations for entire time at Columbia; ranked the 3rd or 4th best teacher of a faculty of 20 members in the earliest days of the department. Primary course taught CSW4701, Artificial Intelligence, consistently one of the largest total enrollments, averaging over 41 students per semester. Advanced Intelligent Systems (former Knowledge-based Expert Systems). Intrusion and Anomaly Detection Systems, an elective in the MS Security track.

Courses Taught at Columbia

- CSW6185 Intrusion and Anomaly Detection Systems, Fall 2004, enrollment 19, Fall 2005 Enrollment 31, Fall 2006 Enrollment 21, Fall 2008 Enrollment 35, Fall 2009 50, Fall 2010, 12.
- CSW4701: Artificial Intelligence, Fall 1990 semester, enrollment 65; Spring 1993 semester, enrollment 58; Fall 1993 semester, enrollment 30; Spring 1994 semester, enrollment 40; Fall 1994 semester, enrollment 32; Spring 1995 semester, enrollment 64; Fall 1995 semester, enrollment 61; Spring 1996, enrollment 53, Spring 2002, enrollment 36, Fall 2002, 66 + 6 CVN; Fall 2003, enrollment 70 + 5 CVN; Spring 2006 Enrollment 62, Spring 2007, Enrollment 52, Spring 2009 70, Spring 2010 48, Spring 2011 56.
- CSW1001: Introduction to Programming. Sections ranged from 30 to 300 students.
- CSW3131: Data Structures. Sections ranged from 50 to 100 students.

- CSW3232: Fundamental Algorithms. 40 students.
- CSW4721: Knowledge-Based Expert Systems. Sections ranged from 8 to 15, to most recently 104 students.
- CSW6721: Knowledge-Based Expert Systems advanced level. 10 students.

Courses Taught at Bell Laboratories

Artificial Intelligence
Compiler Construction

Courses Taught at New York University

Assembler Language Programming
Introduction to Programming

Courses Taught at CUNY Brooklyn College

Programming Languages and Translators
Artificial Intelligence
Data Structures
Introduction to Programming

Professional Societies

American Association for Artificial Intelligence
IEEE
Association of Computing Machinery (ACM)
Special Interest Group on Management of Data (SIGMOD)
Special Interest Group on Artificial Intelligence (SIGART)
Special Interest Group on Computer Architecture (SIGARCH)
New York Academy of Sciences (past)
Sigma Xi Society (past)

Advisory Boards

Advisory Board of the Electrical and Computer Engineering Department of University of Puerto Rico, NSF CISE Grant oversight, 1995-1997.
Scientific Advisory Board, Center for Advanced Technology, Polytechnic University, 1990-1991.
Accreditation Committee, Department of Higher Education, State of Connecticut, 1979.
External thesis reviewer, University of Waterloo, Waterloo, Canada 1989.
External thesis reviewer, University of Melbourne, Australia, 1982.

Service to the Community

Community communications committee for the Ridgewood Council, Village of Ridgewood, Ridgewood, New Jersey, 2000.

Member of Electronic Village committee for the Ridgewood Board of Education, Ridgewood, New Jersey, 1998.
Member of and fund raiser for the Association for Retarded Citizens.

Vice President of the Board of Directors (non-budgetary) of the NJ Association for Retarded Citizens, Bergen/Passaic Unit, 1985.

Member, Special Services Advisory Council to the Board of Education, Ridgewood, New Jersey, 1997-1998.