SALVATORE JOSEPH STOLFO

Salvatorestolfo.com

Curriculum Vitae

As of March 22, 2019

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

Publication H-Index: **80** as of January 2018 (Google Scholar https://scholar.google.com/citations?user=DknsgF8AAAAJ&hl=en)

Honors and Awards (Recent)

- IEEE Fellow 2018 for contributions to machine learning applied to computer security.
- USENIX Security 2017 Distinguish Paper Award, 2017.
- RAID 2017 Award for most influential paper, dating from 2004.
- Aminer.org Most Influential Scholar 2016, https://aminer.org/mostinfluentialscholar/security
- *Popular Science* Award of "What Best of what's new", 2016.
- Member of DNI ISTEG committee, 2016-present, and several National Academy Committees.

Consultant and Advisor to Government (recent)

- National Academies Panel on Army Research Lab evaluation, 2018.
- Member of Intelligence Science and Technology Experts Group (ISTEG), 2015-present.
- Testimony before the DNI Cybersecurity Research Commission, Jan, 2013
- National Academies Panel on Information Science at the Army Research Laboratory, 2012-2014, 2015-2016.
- ODNI/NSA R6 Computational CyberSecurity in Compromised Environments (C3E) Workshop, 2010.

Invited Speaker (recent)

- RAID 2017, Most influential award paper, September 2017.
- ICDM Workshop on Data Mining for Security, Nov 2017.
- ACM CCS Workshop on Cyber Deception, October 2017.
- DHS S&T, Embedded System Insecurity, Mar 2013.
- RSA Conference, Breaking Research Session, Advanced Firmware Security, San Francisco, Feb 2013.

Program Committee Member (recent)

- AAAI19 AICS Workshop on AI for Cyber Security, 2019.
- IEEE Security Development Conference (SecDev) 2018
- RAID 2017
- WRIT 2013, WRIT 2018 (Workshop on Insider Threat, IEEE S&P Symposium) PC
- RAID 2013 PC Chair
- ACM CCS 2012
- RAID 2012 PC Co-Chair

Issued Patents (Recent)

80	10,069,854		Methods, Systems and Media for Evaluating layered Computer Security Products
79	10,061,753		Systems and methods for content extraction from a mark-up language text accessible at an internet domain
78	10,038,704		Systems and methods for correlating and distributing intrusion alert information among collaborators
77	10,002,249		Systems, methods, and media for outputting data based on anomaly detection
76	9,996,694		Unsupervised detection of anomalous processes using hardware features
75	9,971,891		Methods, systems, and media for detecting covert malware
74	9,870,455		System Level User Behavior Biometrics using feature extraction and modeling
73	**9,654,478**		Methods, media and systems for securing communications between a first node and a second node
72	**9,576,127**		Methods, media, and systems for detecting attack on a digital processing device
71	**9,544,322**		Systems, methods, and media protecting a digital data processing device from attack
70	**9,519,778**		Systems, methods, and media for outputting a dataset based upon anomaly detection
69	**9,501,639**		Methods, systems, and media for baiting inside attackers
68	**9,497,203**		System and methods for model generation for detecting intrusion in computer systems
67	**9,450,979**		Methods, media, and systems for detecting an anomalous sequence of function calls
66	**9,419,981**		Methods, media, and systems for securing communications between a first node and a second node

Books and Journal Issues (Recent)

1. *Anomaly Detection as a Service: Challenges, Advances, and Opportunities, Synthesis Lectures on Security, Privacy, and Trust,* Danfend Yao, Xiaokui Shu, Long Cheng, and Salvatore J Stolfo, October 2017. Morgan & Claypool, (https://doi.org/10.2200/S00800ED1V01Y201709SPT022)
2. *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.*
3. *IEEE Security and Privacy Special Issue on the Science of Security*, co-Editor, May 2011.
4. *IEEE Security and Privacy Special Issue on Privacy-Preserving Sharing of Sensitive Information*, co-Editor, 2009-2010.

Book Chapters - Peer Refereed (Recent)

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.

Journal and Periodical Publications - Refereed (Recent)

1. Active Authentication using File System Decoys and User Behavior Modeling: Results of a Large Scale Study, J. Voris, Y. Song, M. Ben Salem, S. Hershkop, and S. J. Stolfo, Journal of Computers and Society (Spafford, Ed.), Elsevier, 2018.
2. 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.

3. 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, 2014.
4. 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.
5. Usable Secure Private Search, (with B. Vo, M. Raykova, A Cui, T. Malkin, and S. Bellovin), *IEEE Security and Privacy*, 2011.

Conference and Symposia Proceedings – Refereed (Recent)

1. CLKSCREW: Exposing the Perils of Security-Oblivious Energy Management, Adrian Tang, Simha Sethumadhavan and Salvatore J Stolfo, Usenix Security, 2017. (Usenix Security Distinguished Paper Award.)
2. NEZHA: Efficient Domain-independent Differential Testing, (with Th eofilos Petsios, Adrian Tang, Salvatore Stolfo, Angelos D. Keromytis and Suman Jana. Proc. IEEE Security and Privacy, 2017.
3. You are what you use: An Initial Study of Authenticating Mobile Users via Application Usage, Jonathan Voris, Malek Ben Salem, Yingbo Song and Salvatore J Stolfo, 8th EAI Int Conference on Mobile Computing, Applications and Service, Mobicase 2016.
4. Using Diversity to Harden Multithreaded Programs Against Exploitation, (with David Tagatac and Michalis Polychronakis), IEEE Int. Conference on High Performance and Smart Computing, IEEE HPC, 2016.
5. Heisenbyte, Thwarting Memory Disclosure Attacks using Destructive Code Reads (with Adrian Tang and Simha Sethumadhavan), ACM CCS 2015.

Workshop Papers Peer Reviewed

1. Simulated User Bots: Real Time Testing of Insider Threat Detection Systems, Preetam Dutta, Gabriel Ryan, Aleksander Zieba and Salvatore Stolfo, IEEE Symp on Security and Privacy, Workshop on Research for Insider Threat, March 2018.
2. 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.
3. Model Aggregation for Distributed Content Anomaly Detection, Sean Whalen, Nathaniel Boggs and Sal Stolfo, AI Security Workshop, CCS, 2014.
4. 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.
5. 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.

Technical Presentations (Recent)

1. A brief history of Symbiote Defense, MIT/CSAIL, NYU, UPenn, Datmouth, October 2017.
2. Deception Security and Active Authentication: How to Protect your Data For real, Dartmouth, Nov 2017.
3. Deception Security and Active Authentication, First International Workshop on Cyber Deception and Defenses, 2017.
4. RSA 2015, Hot Research Topics: Symbiote Technology, Decoy Technology, April 2015.
5. Office of the Secretary of the Air Force, Embedded Insecurity, January 2015.

PhD Students

Graduated 31 Students. (10 Academia, 21 Industry)