Mihai Christodorescu

1011 Curtner Ave, San Jose, CA, USA
+1 608-695-6271
mihaic@gmail.com
https://www.christodorescu.org/

Curriculum Vitæ

Research Interests

I am interested in fundamental approaches to *computer security and privacy* problems by combining methods from multiple domains—programming languages, machine learning, behavioral modeling, and formal methods. My past and present projects have addressed Internet-scale security analysis of networks, systems, and software, and whole-system security hardening for both cloud and mobile endpoints.

Education

2003–2007	Ph.D. in Computer Sciences, August 2007. University of Wisconsin, Madison, WI, USA. Dissertation: *Behavior-based Malware Detection.* Adviser: Prof. Somesh Jha.
1999–2000, 2001–2002	M.S. in Computer Sciences, Dec. 2002. University of Wisconsin, Madison, WI, USA. Adviser: Prof. Somesh Jha.
1996–1999	B.S. (High Honors) in Computer Science, May 1999. University of California, Santa Barbara, CA, USA.

Research Experience

2013–present	*Senior Research Staff Engineer* Qualcomm Research Silicon Valley, Santa Clara, CA, USA Mobile security, network and web security via unsupervised machine learning, usable web privacy
2007–2013	*Research Staff Member*, Security Analysis Lab IBM T.J. Watson Research Center, Hawthorne, NY, USA Virtual-machine introspection, scalable malware analysis, botnet detection, cybersecurity and situational awareness, and cloud security
2001–2007	*Research Assistant*, Wisconsin Safety Analyzer (WiSA) project University of Wisconsin, Madison, WI, USA Detection of malicious behavior in obfuscated binary code, using static program analysis and formal methods
2000	*Research Assistant*, Paradyn project University of Wisconsin, Madison, WI, USA Reentrant binary instrumentation of running processes

Publications

Books

1. Mihai Christodorescu, Somesh Jha, Douglas Maughan, Dawn Song, and Cliff Wang, editors. *Malware Detection*, volume 27 of *Advances in Information Security*. Springer-Verlag, October 2006.

Conference Publications

2. Man-Ki Yoon, Negin Salajegheh, Yin Chen, and Mihai Christodorescu. PIFT: predictive information-flow tracking. In *Proceedings of the Twenty-First International Conference on Architectural Support for Programming Languages and Operating Systems, ASPLOS '16, Atlanta, GA, USA, April 2-6, 2016*, pages 713–725, 2016. doi: 10.1145/2872362.2872403.

3. Man-Ki Yoon, Mihai Christodorescu, Lui Sha, and Sibin Mohan. The DragonBeam framework: Hardware-protected security modules for in-place intrusion detection. In *Proceedings of the 9th ACM International on Systems and Storage Conference, SYSTOR 2016, Haifa, Israel, June 6-8, 2016*, pages 1:1–1:12, 2016. doi: 10.1145/2928275.2928290.

4. William Melicher, Mahmood Sharif, Joshua Tan, Lujo Bauer, Mihai Christodorescu, and Pedro Giovanni Leon. (Do Not) Track Me Sometimes: Users' contextual preferences for web tracking. *PoPETs*, 2016(2):135–154, 2016.

5. Man-Ki Yoon, Sibin Mohan, Jaesik Choi, Mihai Christodorescu, and Lui Sha. Learning execution contexts from system call distribution for anomaly detection in smart embedded systems. In *Proceedings of the 2nd ACM/IEEE International Conference on Internet-of-Things Design and Implementation (IoTDI 2017)*, April 2017.

6. Man-Ki Yoon, Sibin Mohan, Jaesik Choi, Mihai Christodorescu, and Lui Sha. Intrusion detection using execution contexts learned from system call distributions of real-time embedded systems. *CoRR*, abs/1501.05963, 2015. URL http://arxiv.org/abs/1501.05963.

7. Rui Han, Alejandro Mesa, Mihai Christodorescu, and Saman A. Zonouz. Troguard: context-aware protection against web-based socially engineered trojans. In *Proceedings of the 30th Annual Computer Security Applications Conference, ACSAC 2014, New Orleans, LA, USA, December 8-12, 2014*, pages 66–75, 2014. doi: 10.1145/2664243.2664270. URL http://doi.acm.org/10.1145/2664243.2664270.

8. Douglas Lee Schales, Mihai Christodorescu, Xin Hu, Jiyong Jang, Josyula R. Rao, Reiner Sailer, Marc Ph. Stoecklin, Wietse Venema, and Ting Wang. Stream computing for large-scale, multi-channel cyber threat analytics. In *Proceedings of the 15th IEEE International Conference on Information Reuse and Integration, IRI 2014, Redwood City, CA, USA, August 13-15, 2014*, pages 8–15, 2014. doi: 10.1109/IRI.2014.7051865. URL http://dx.doi.org/10.1109/IRI.2014.7051865.

9. Vern Paxson, Mihai Christodorescu, Mobin Javed, Josyula Rao, Reiner Sailer, Douglas Schales, Marc Ph. Stoecklin, Kurt Thomas, Wietse Venema, and Nicholas Weaver. Practical comprehensive bounds on surreptitious communication over dns. In *Proceedings of the 22nd USENIX Conference on Security*, SEC'13, pages 17–32, Berkeley, CA, USA, 2013. USENIX Association. ISBN 978-1-931971-03-4. URL http://dl.acm.org/citation.cfm?id=2534766.2534769.

10. Pedro Giovanni Leon, Blase Ur, Yang Wang, Manya Sleeper, Rebecca Balebako, Richard Shay, Lujo Bauer, Mihai Christodorescu, and Lorrie Faith Cranor. What matters to users?: Factors that affect users' willingness to share information with online advertisers. In *Proceedings of the Ninth Symposium on Usable Privacy and Security*, SOUPS '13, pages 7:1–7:12, New York, NY, USA, 2013. ACM. ISBN 978-1-4503-2319-2. doi: 10.1145/2501604.2501611. URL http://doi.acm.org/10.1145/2501604.2501611.

11. Shakeel Butt, Vinod Ganapathy, Arati Baliga, and Mihai Christodorescu. Monitoring data structures using hardware transactional memory. In *Proceedings of the 2nd International Conference on Runtime Verification (RV'11)*, volume 7186 of *Lecture Notes in Computer Science*, pages 345–359, San Francisco, CA, USA, September 27–30, 2011. Springer. ISBN 978-3-642-29859-2.

Publications (continued)

12. Matthew Fredrikson, Mihai Christodorescu, and Somesh Jha. Dynamic behavior matching: A complexity analysis and new approximation algorithms. In Nikolaj Bjørner and Viorica Sofronie-Stokkermans, editors, *Proceedings of the 23rd International Conference on Automated Deduction (CADE'11)*, volume 6803 of *Lecture Notes in Computer Science*, pages 252–267. Springer, July 31–August 5, 2011. ISBN 978-3-642-22437-9. doi: 10.1007/978-3-642-22438-6.

13. Andrea Lanzi, Davide Balzarotti, Christopher Kruegel, Mihai Christodorescu, and Engin Kirda. AccessMiner: using system-centric models for malware protection. In *Proceedings of the 17th ACM Conference on Computer and Communications Security (CCS'10)*, pages 399–412, New York, NY, USA, 2010. ACM Press. ISBN 978-1-4503-0245-6. doi: 10.1145/1866307.1866353.

14. Matt Fredrikson, Somesh Jha, Mihai Christodorescu, Reiner Sailer, and Xifeng Yan. Synthesizing near-optimal malware specifications from suspicious behaviors. In *Proceedings of the 2010 IEEE Symposium on Security and Privacy (S&P'10)*, pages 45–60, May 2010. doi: 10.1109/SP.2010.11.

15. Mihai Christodorescu, Reiner Sailer, Douglas Lee Schales, Daniele Sgandurra, and Diego Zamboni. Cloud security is not (just) virtualization security: a short paper. In Radu Sion and Dawn Song, editors, *Proceedings of the 2009 ACM Cloud Computing Security Workshop (CCSW'09)*, pages 97–102. ACM Press, November 13, 2009. ISBN 978-1-60558-784-4. doi: 10.1145/1655008.1655022.

16. Chen Chen, Cindy X Lin, Matt Fredrikson, Mihai Christodorescu, Xifeng Yan, and Jiawei Han. Mining graph patterns efficiently via randomized summaries. *Proceedings of the VLDB Endowment*, 2(1):742–753, August 2009. ISSN 2150-8097.

17. Mihai Christodorescu. Private use of untrusted web servers via opportunistic encryption. In *Proceedings of the Web 2.0 Security & Privacy Workshop 2008 (W2SP'08)*, May 2008.

18. Lorenzo Martignoni, Mihai Christodorescu, and Somesh Jha. Omniunpack: Fast, generic, and safe unpacking of malware. In *Proceedings of the 23rd Annual Computer Security Applications Conference (ACSAC'07)*, pages 431–441. IEEE Computer Society, December 10–14, 2007.

19. Mihai Christodorescu, Christopher Kruegel, and Somesh Jha. Mining specifications of malicious behavior. In *Proceedings of the 6th Joint Meeting of the European Software Engineering Conference and the ACM SIGSOFT Symposium on the Foundations of Software Engineering (ESEC/FSE'07)*, pages 5–14, New York, NY, USA, 2007. ACM Press. ISBN 978-1-59593-811-4. doi: 10.1145/1287624.1287628.

20. Mihai Christodorescu, Somesh Jha, Johannes Kinder, Stefan Katzenbeisser, and Helmut Veith. Software transformations to improve malware detection. *Journal in Computer Virology*, 3(4):253–265, 2007. doi: 10.1007/s11416-007-0059-8.

21. Mila Dalla Preda, Mihai Christodorescu, Somesh Jha, and Saumya Debray. A semantics-based approach to malware detection. In *Proceedings of the 34th Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages (POPL'07)*, pages 377–388, New York, NY, USA, January 17–19, 2007. ACM Press. doi: 10.1145/1190216.1190270.

22. Jonathon Giffin, Mihai Christodorescu, and Louis Kruger. Strengthening software self-checksumming via self-modifying code. In *Proceedings of the 21st Annual Computer Security Applications Conference (ACSAC'05)*, pages 18–27, Tucson, AZ, USA, December 5–9, 2005. Applied Computer Associates, IEEE Computer Society.

23. Shai Rubin, Mihai Christodorescu, Vinod Ganapathy, Jonathon T. Giffin, Louis Kruger, Hao Wang, and Nicholas Kidd. An auctioning reputation system based on anomaly detection. In *Proceedings of the 12th ACM Conference on Computer and Communications Security (CCS'05)*, pages 270–279, New York, NY, USA, 2005. ACM Press. ISBN 1-59593-226-7. doi: 10.1145/1102120.1102156.

24. Mihai Christodorescu, Nicholas Kidd, and Wen-Han Goh. String analysis for x86 binaries. In *Proceedings of the 6th ACM SIGPLAN-SIGSOFT Workshop on Program Analysis for Software Tools and Engineering (PASTE'05)*, Lisbon, Portugal, September 5–6, 2005. ACM Press.

Publications (continued)

25. Mihai Christodorescu, Somesh Jha, Sanjit A. Seshia, Dawn Song, and Randal E. Bryant. Semantics-aware malware detection. In *Proceedings of the IEEE Symposium on Security and Privacy (S&P'05)*, pages 32–46, Oakland, CA, USA, May 8–11, 2005. IEEE Computer Society.

26. Mihai Christodorescu and Somesh Jha. Testing malware detectors. In *Proceedings of the ACM SIGSOFT International Symposium on Software Testing and Analysis (ISSTA'04)*, pages 34–44, Boston, MA, USA, July 11–14, 2004. ACM SIGSOFT, ACM Press.

27. Mihai Christodorescu and Somesh Jha. Static analysis of executables to detect malicious patterns. In *Proceedings of the 12th USENIX Security Symposium (Security'03)*, pages 169–186, Washington, DC, USA, August 4–8, 2003. USENIX Association.

Journal Publications

28. Marc Ph. Stoecklin, Kapil Singh, Larry Koved, Xin Hu, Suresh N. Chari, Josyula R. Rao, P.-C. Cheng, Mihai Christodorescu, Reiner Sailer, and Douglas Lee Schales. Passive security intelligence to analyze the security risks of mobile/BYOD activities. *IBM Journal of Research and Development*, 60(4):9, 2016. doi: 10.1147/JRD.2016.2569858.

29. Mila Dalla Preda, Mihai Christodorescu, Somesh Jha, and Saumya K. Debray. A semantics-based approach to malware detection. *ACM Transactions on Programming Languages and Systems (TOPLAS)*, 30(5), 2008.

30. Barton P. Miller, Mihai Christodorescu, Robert Iverson, Tevfik Kosar, Alexander Mirgorodskii, and Florentina Popovici. Playing inside the black box: Using dynamic instrumentation to create security holes. *Parallel Processing Letters*, 11(2/3):267–280, June/September 2001.

Invited Publications

31. Somesh Jha, Matthew Fredrikson, Mihai Christodorescu, Reiner Sailer, and Xifeng Yan. Synthesizing near-optimal malware specifications from suspicious behaviors. In *8th International Conference on Malicious and Unwanted Software: "The Americas", MALWARE 2013, Fajardo, PR, USA, October 22-24, 2013*, pages 41–50, 2013. doi: 10.1109/MALWARE.2013.6703684. URL http://dx.doi.org/10.1109/MALWARE.2013.6703684.

32. Mihai Christodorescu, Somesh Jha, and Christopher Kruegel. Mining specifications of malicious behavior. In Gautam Shroff, Pankaj Jalote, and Sriram K. Rajamani, editors, *Proceedings of the 1st Annual India Software Engineering Conference (ISEC'08)*, pages 5–14. ACM Press, February 19–22, 2008. ISBN 978-1-59593-917-3.

33. Mihai Christodorescu and Vinod Ganapathy. Dynamic analysis. In Henk C. A. van Tilborg and Sushil Jajodia, editors, *Encyclopedia of Cryptography and Security, 2nd ed*, pages 365–367. Springer, 2011. ISBN 978-1-4419-5905-8. doi: 10.1007/978-1-4419-5906-5_836.

34. Mihai Christodorescu, Matthew Fredrikson, Somesh Jha, and Jonathon Giffin. End-to-end software diversification of internet services. In Sushil Jajodia, Anup K. Ghosh, Vipin Swarup, Cliff Wang, and Sean X. Wang, editors, *Moving Target Defense*, volume 54 of *Advances in Information Security*, pages 117–130. Springer New York, 2011. ISBN 978-1-4614-0977-9. doi: 10.1007/978-1-4614-0977-9_7.

35. Matt Fredrikson, Mihai Christodorescu, Jonathon Giffin, and Somesh Jha. A declarative framework for intrusion analysis. In Sushil Jajodia, Peng Liu, Vipin Swarup, and Cliff Wang, editors, *Cyber Situational Awareness*, volume 46 of *Advances in Information Security*, pages 179–200. Springer US, 2010. ISBN 978-1-4419-0140-8. doi: 10.1007/978-1-4419-0140-8_9.

36. Mihai Christodorescu and Shai Rubin. Can cooperative intrusion detectors challenge the base-rate fallacy? In Mihai Christodorescu, Somesh Jha, Douglas Maughan, Dawn Song, and Cliff Wang, editors, *Malware Detection*, volume 27 of *Advances in Information Security*, pages 193–209, August 2005. This edited volume represents the proceedings of the 2005 ARO-DHS Special Workshop on Malware Detection, Aug. 10–11, 2005, Arlington, VA, USA.

Publications (continued)

Technical Reports

37. Douglas L. Schales, Mihai Christodorescu, Josyula R. Rao, Reiner Sailer, Marc Ph. Stoecklin, and Wietse Venema. Stream computing for large-scale, multi-channel cyber threat analytics: Architecture, implementation, deployment, and lessons learned. Technical Report RC25172, IBM T.J. Watson Research Center, 2011.

38. Douglas L. Schales, Mihai Christodorescu, Mitchell A. Cohen, Josyula R. Rao, and Reiner Sailer. Calypsos: An experimentation-friendly, real-time, and scalable cybersecurity analytics engine. Technical Report RC25153, IBM T.J. Watson Research Center, 2011.

39. Mihai Christodorescu, Johannes Kinder, Somesh Jha, Stefan Katzenbeisser, and Helmut Veith. Malware normalization. Technical Report 1539, University of Wisconsin, Madison, WI, USA, November 2005.

40. Jonathon T. Giffin, Mihai Christodorescu, and Louis Kruger. Strengthening software self-checksumming via self-modifying code. Technical Report 1531, University of Wisconsin, Madison, WI, USA, September 2005.

41. Tevfik Kosar, Mihai Christodorescu, and Robert Iverson. Opening pandora's box: Using binary code rewrite to bypass license checks. Technical Report 1479, University of Wisconsin, Madison, WI, USA, April 2003.

42. Mihai Christodorescu and Somesh Jha. SAFE: Static analysis for executables. Technical Report 1467, University of Wisconsin, Madison, WI, USA, February 2003.

Patents

43. Rajarshi Paul Gupta, Mihai Christodorescu, Vinay Sridhara, Mastooreh Salajegheh, and Andres Valencia. Adaptive observation of behavioral features on a mobile device. U.S. Patent 9 330 257, May 3, 2016.

44. Rajarshi Paul Gupta, Mihai Christodorescu, Yin Che Chen, Vinay Sridhara, Mastooreh Salajegheh, and Man Ki Yoon. Data flow tracking via memory monitoring. U.S. Patent 9 519 533, December 13, 2016.

45. Ting Z. Wang, Reiner Sailer, Douglas Lee Schales, Mihai Christodorescu, Marc Stoecklin, and Xin Hu. Distributed feature collection and correlation engine. U.S. Patent 9 489 426, November 8, 2016.

46. Ting Z. Wang, Reiner Sailer, Douglas Lee Schales, Mihai Christodorescu, Marc Stoecklin, and Xin Hu. Distributed feature collection and correlation engine. U.S. Patent 9 495 420, November 15, 2016.

47. Ting Z. Wang, Reiner Sailer, Douglas Lee Schales, Mihai Christodorescu, Marc Stoecklin, Xin Hu, and Andrew M. White. Identification and classification of web traffic inside encrypted network tunnels. U.S. Patent 9 491 078, November 8, 2016.

48. Rajarshi Paul Gupta, Mihai Christodorescu, Vinay Sridhara, Kassem Fawaz, and David Jerome Fiala. Pre-identifying probable malicious rootkit behavior using behavioral contracts. U.S. Patent 9 323 929, April 26, 2016.

49. Dimitrios Pendarakis, Mihai Christodorescu, and Kapil K. Singh. Protection of user data in hosted application environments. U.S. Patent 9 245 126, January 26, 2016.

50. Dimitrios Pendarakis, Mihai Christodorescu, and Kapil K. Singh. Protection of user data in hosted application environments. U.S. Patent 9 430 653, August 30, 2016.

51. Ting Z. Wang, Reiner Sailer, Douglas Lee Schales, Mihai Christodorescu, and Marc Stoecklin. User identification using multifaceted footprints. U.S. Patent 9 251 328, February 2, 2016.

Publications (continued)

52. Josyula R. Rao, Mitchell A. Cohen, Lisa D. Amini, Olivier Verscheure, Reiner Sailer, Douglas Lee Schales, Mihai Christodorescu, Srinivasan Parthasarathy, and Wietse Z. Venema. Adaptive cybersecurity analytics. U.S. Patent 9 032 521, May 12, 2015.

53. Ting Z. Wang, Reiner Sailer, Douglas Lee Schales, Mihai Christodorescu, Marc Stoecklin, Xin Hu, and Andrew M. White. Identification and classification of web traffic inside encrypted network tunnels. U.S. Patent 9 100 309, August 4, 2015.

54. Ting Z. Wang, Reiner Sailer, Douglas Lee Schales, Mihai Christodorescu, Marc Stoecklin, Xin Hu, and Andrew M. White. Identification and classification of web traffic inside encrypted network tunnels. U.S. Patent 9 106 536, August 11, 2015.

55. Rajarshi Paul Gupta, Mihai Christodorescu, and David Jerome Fiala. Lightweight data-flow tracker for realtime behavioral analysis using control flow. U.S. Patent 9 158 604, October 13, 2015.

56. Andrew Everett Davidson, Reiner Sailer, Mihai Christodorescu, and Wietse Z. Venema. Malware detection via network information flow theories. U.S. Patent 8 935 782, January 13, 2015.

57. Josyula R. Rao, Reiner Sailer, Douglas Lee Schales, and Mihai Christodorescu. Method and apparatus for detecting unauthorized bulk forwarding of sensitive data over a network. U.S. Patent 8 938 511, January 20, 2015.

58. Josyula R. Rao, Reiner Sailer, Douglas Lee Schales, and Mihai Christodorescu. Method and apparatus for detecting unauthorized bulk forwarding of sensitive data over a network. U.S. Patent 8 972 510, March 3, 2015.

59. Rajarshi Paul Gupta, Mihai Christodorescu, Vinay Sridhara, and Kassem Fawaz. Method and system for performing behavioral analysis operations in a mobile device based on application state. U.S. Patent 9 147 072, September 29, 2015.

60. Reiner Sailer, Douglas Lee Schales, Dimitrios Pendarakis, Mihai Christodorescu, and Najwa Aaraj. Optimizing performance of integrity monitoring. U.S. Patent 8 949 797, February 3, 2015.

61. Dimitrios Pendarakis, Mihai Christodorescu, and Kapil K. Singh. Protection of user data in hosted application environments. U.S. Patent 9 098 709, August 4, 2015.

62. Ajay Mohindra, Ashish Kundu, and Mihai Christodorescu. System and method for protection from buffer overflow vulnerability due to placement new constructs in C++. U.S. Patent 9 069 970, June 30, 2015.

63. Ajay Mohindra, Ashish Kundu, and Mihai Christodorescu. System and method for protection from buffer overflow vulnerability due to placement new constructs in c++. U.S. Patent 9 081 966, July 14, 2015.

64. Ting Z. Wang, Reiner Sailer, Douglas Lee Schales, Mihai Christodorescu, and Marc Stoecklin. User identification using multifaceted footprints. U.S. Patent 9 003 025, April 7, 2015.

65. Ting Z. Wang, Reiner Sailer, Douglas Lee Schales, Mihai Christodorescu, Marc Stoecklin, and Dmytro Korzhyk. Predicting attacks based on probabilistic game-theory. U.S. Patent 8 863 293, October 14, 2014.

66. Mihai Christodorescu and Somesh Jha. Method and apparatus to detect malicious software. U.S. Patent 7 739 737, June 15, 2010.

67. Mihai Christodorescu, Somesh Jha, Johannes Kinder, Stefan Katzenbeisser, and Helmut Veith. Malware normalization. Patent application in progress, 2006.

Selected Awards and Achievements

2007 Distinguished ACM SIGSOFT paper award at the
6th Joint Meeting of the European Software Engineering Conference and the ACM SIGSOFT Symposium on the Foundations of Software Engineering (ESEC/FSE'07), 2007, Dubrovnik, Croatia. (See publication 19.)

2004 Distinguished ACM SIGSOFT paper award at
International Symposium on Software Testing and Analysis (ISSTA'04), 2004, Boston, MA, USA. (See publication 26.)

1996–1999 Dean's honor list at University of California, Santa Barbara.

Mentoring

2017 Man-Ki Yoon (UIUC)
Ph.D. committee

2016–2017 Utsav Banerjee, Chiraag Juvekar (MIT)
Qualcomm Innovation Fellowship 2016 winners
"Hardware Acceleration for Mobile Computing on Encrypted Data"

2016 Drew Davidson (University of Wisconsin – Madison)
Ph.D. committee

2016 Ahmet Buyyukayhan (NEU)
summer intern

2015 Rui Han (UMiami)
Ph.D. committee

2015 Mikhail Kazdagli (UT Austin)
summer intern

2014 Man-Ki Yoon (UIUC)
summer intern

2013–2014 Fardin Abdi, Man-Ki Yoon (UIUC)
Qualcomm Innovation Fellowship 2013 winners
"Behavior Pattern Inspection: A New Approach for Securing Real-Time Embedded Systems"

2013 David J. Fiala (NCSU)
summer intern

2012 Gianluca Stringhini (UCSB)
summer intern

Andrew White (UNC)
summer intern

2011 Dmytro Korzhyk (Duke)
summer intern

Mentoring (continued)

2010 Drew Davidson (University of Wisconsin – Madison)
summer intern

2009 Richard Chang (UT Austin)
summer intern

2008 Najwa Aaraj (Princeton)
summer intern

Matt Fredrikson (University of Wisconsin – Madison)
summer intern

Teaching Experience

2006 Teaching Assistant for "Introduction to Information Security."
Graduate and senior-undergraduate level course. Instructor: Somesh Jha. (University of Wisconsin, Madison, Computer Sciences course 642, Spring 2006)

Workshop on "The Act of Teaching: Theatrical Tips for Teachers."
Presented by Nancy Houfek, head of voice and speech at Harvard's Institute for Advanced Theatre Training. Organized by the UW Delta Research Teaching and Learning Community. (Sept. 2006)

2003–2006 Invited Lecturer on malicious code and attack methods. Mentor for several course projects. Course: "Introduction to Information Security." Instructor: Somesh Jha. (University of Wisconsin, Madison, Computer Sciences course 642, Spring semester)

2004 Workshop on "Creating a Teaching and Learning Philosophy."
Organized by the UW Delta Research Teaching and Learning Community. (Nov. 2004)

2001 Mentor for two course projects.
Course: "Analysis of Software Artifacts." Instructor: Somesh Jha. (University of Wisconsin, Madison, Computer Sciences course 706, Fall 2001)

1999 Teaching Assistant for "Java for C++ programmers" and "C++ for Java programmers."
Junior-undergraduate level. Instructor: Susan Horwitz. (University of Wisconsin, Madison, Computer Sciences course 368, Fall 1999)

Professional Activities

Organizer

International Workshop on Building Analysis Datasets and Gathering Experience Returns for Security (BADGERS): 2014, 2015.

IBM Student Workshop for Frontiers of Cloud Computing (F2C2), 2011, Hawthorne, NY, USA.

IBM Student Workshop for Frontiers of Cloud Computing (F2C2), 2010, Hawthorne, NY, USA.

Professional Activities (continued)

IBM Research–Princeton University Security & Privacy Day, 2007, Princeton, NJ, USA.

Program Committee Member

Conferences:

ACM Cloud Computing Security Workshop (CCSW): 2010, 2011, 2012, 2016.
ACM Conference on Computer and Communications Security (CCS): 2008, 2009, 2010, 2012.
ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM): 2014, 2016.
ACM CCS Workshop on Recurring Malcode (WORM): 2007.
ACM International Workshop on IoT Privacy, Trust, and Security (IoTPTS): 2015, 2016, 2017.
ACM Symposium on Information, Computer and Communications Security (ASIACCS): 2012, 2016.
Annual Computer Security Applications Conference (ACSAC): 2012.
Building Analysis Datasets and Gathering Experience Returns for Security (BADGERS): 2011, 2012.
Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA): 2012.
Conference on Principles of Security and Trust (POST): 2013.
European Workshop on System Security (EuroSec): 2010, 2011, 2012.
International Conference on Information Systems Security (ICISS): 2010, 2011.
IEEE International Conference on Communications' Communications and Information System Security Symposium (IEEE ICC CISS): 2009, 2011.
IEEE International Conference on Communications' Information and Network Security (IEEE ICC INS): 2008.
IFIP International Information Security Conference (IFIP SEC): 2010.
Innovations in Mobile Privacy and Security workshop (IMPS): 2016, 2017.
International Conference on Malicious and Unwanted Software (Malware): 2008, 2011.
International Conference on Security and Privacy in Communication Networks (SECURECOMM): 2011, 2012.
International Symposium on Recent Advances in Intrusion Detection (RAID): 2009, 2010, 2012, 2017.
International Workshop on Secure Internet of Things (SIoT): 2015.
International Workshop on Software Engineering for Secure Systems (SESS): 2008, 2009, 2010, 2011, 2012.
Mobile Security Technologies Workshop (MoST): 2015, 2016, 2017.
Network & Distributed System Security Symposium (NDSS): 2009, 2010, 2011, 2014.
International Conference on Security and Privacy in Communication Networks (SECURECOMM): 2015.
USENIX Annual Technical Conference (USENIX ATC): 2017.
USENIX Security Symposium (USENIX Sec): 2012.
USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET): 2012.
Web 2.0 Security & Privacy Workshop (W2SP): 2013.
Workshop on Program Protection and Reverse Engineering (PPREW): 2012, 2014, 2015.

Professional Activities (continued)

External Reviewer

Journals:
ACM Computing Surveys: 2015, 2016.
ACM SIGOPS Operating Systems Review (OSR): 2008.
ACM Transactions on Information and System Security (TISSEC): 2007, 2010.
ACM Transactions on Internet Technology (TOIT): 2004.
Communications of the ACM (CACM): 2005 (issue on spyware), 2011.
Computer Journal: 2011.
Engineering Applications of Artificial Intelligence: 2014.
IEEE Micro: 2014.
IEEE Transactions of Cloud Computing (TCC): 2014.
IEEE Transactions on Information Forensics and Security (TIFS): 2009, 2011, 2015.
IEEE Transactions on Dependable and Secure Computing (TDSC): 2010, 2013.
IEEE Transactions on Knowledge and Data Engineering (TKDE): 2009.
IEEE/ACM Transactions on Networking (ToN): 2009.
Journal of Computer Security (JCS): 2006, 2009.

Conferences:
ACM Conference on Computer and Communication Security (CCS): 2005, 2006, 2014.
ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM): 2013.
Annual Computer Security Applications Conference (ACSAC): 2006, 2008.
Computer Security Foundations Workshop/Symposium (CSF): 2008.
European Symposium on Research in Computer Security (ESORICS): 2009.
Foundations of Computer Security Workshop (FCS): 2001.
IEEE/IFIP International Conference on Dependable Systems and Networks (DSN): 2011.
IEEE/IFIP Network Operations and Management Symposium (NOMS): 2012.
IEEE International Conference on Communications' Information and Network Security (IEEE ICC INS): 2008.
IEEE Security & Privacy Symposium ("Oakland"): 2009, 2012.
International World Wide Web Conference (WWW): 2005.
International Conference on Computer Aided Verification (CAV): 2005.
LCI International Conference on Clusters: 2006.
Mobile Security Technologies Workshop (MoST): 2014.
Network and Distributed System Security Symposium (NDSS): 2005, 2007.
Recent Advances in Intrusion Detection (RAID): 2005, 2009.
Software Engineering for Secure Systems (SESS): 2005.
Symposium on Requirements Engineering for Information Security (SREIS): 2002.
USENIX Annual Technical Conference: 2004.
USENIX Security Symposium: 2005, 2006, 2008, 2009, 2010.
Workshop on Rapid Malcode (WORM): 2005.

Invited Talks and Panels

Cybersecurity Panel, Feb. 13, 2012, University of Pennsylvania, Philadelphia, PA, USA.

Seminar on Analysis of Executables: Benefits and Challenges, Jan. 29–Feb. 3, 2012, Schloss Dagstuhl, Wadern, Germany.

ARO Workshop on Moving Target Defense, Oct. 25–26, 2010, Fairfax, VA, USA.

2nd FORWARD Workshop, May 4–5, 2009, Saint-Jean-Cap-Ferrat, France.

Computing in the Cloud workshop, Jan. 14–15, 2008, Princeton University, NJ, USA.

Professional Activities (continued)

Workgroup on Future Malware Threats, 3rd workshop of the ARDA Malware Roadmap series, Sept. 20–22, 2005, Salt Lake City, UT, USA.

Workgroup on Malware Detection, ARO–DHS Special Workshop on Malware Detection, Aug. 10–11, 2005, Arlington, VA, USA.

ONR CIP/SW MURI Project Review for Dr. James Whittaker (FIT), "Runtime Neutralization of Malicious Mobile Code," Feb. 2005.

Software Protection Compilation Workshop, Nov. 12–13, 2003, Washington, DC, USA.

Academic Activities

Member of the DIMACS Special Focus on Cybersecurity organizing committee, 2011–2013.

Member of the New York Region Security & Privacy Day advisory board, 2011–present.

Member of the Graduate Admissions Committee at the Department of Computer Sciences, University of Wisconsin, Madison, 2002.

Organizer of the computer security seminar at the Department of Computer Sciences, University of Wisconsin, Madison, 2001–2006.

Coordinator of the computer security reading group at the Department of Computer Sciences, University of Wisconsin, Madison, 2001–2006.

Industry Impact

2006–2007 Co-founder of Novashield, a Madison, WI, provider of behavior-based malware-detection products.

2005–2006 Transfer of technology for "Effective Malware Detection Through Static Analysis" to Grammatech, Inc., Ithaca, NY. (ONR STTR Phases I and II)

2006 Attended TrendMicro's "Meeting of the Minds," Feb. 13, 2006, Las Vegas, NV, USA.

Professional Experience

2015–present *Senior Staff Engineer*, Qualcomm Research Silicon Valley, Santa Clara, CA, USA.

- Led team to design hardware mechanisms for probabilistic information-flow tracking
- Led team to design and prototype scalable, unsupervised network security analytics
- Coordinated lab-wide university relations program

2013–2015 *Staff Engineer*, Qualcomm Research Silicon Valley, Santa Clara, CA, USA.

- Designed and prototyped low-power behavioral analytics for malware detection
- Designed Android app splitting security mechanism

Professional Experience (continued)

2007–2013 *Research Staff Member*, IBM T.J. Watson Research Center, Hawthorne, NY, USA.

- Designed and prototyped scalable, real-time security analytics for network security
- Designed and prototyped security analytics for virtualized environments
- Researched joint host and network attack detection
- Designed attack-resilient malware analyses based on graph mining
- Prototyped detection of stealthy DNS tunnels
- Designed and prototyped trojan detection based on perceived behavioral mismatch
- Designed detection of malware lateral expansion via traffic causality inference
- Designed scalable encrypted classification of encrypted web traffic

2006–2007 *Principal Scientist*, Novashield, Madison, WI, USA.

- Spearheaded tech transfer of semantics-aware malware detector

2000–2001 *Senior Software Engineer*, Yodlee, Inc., Redwood City, CA, USA.

- Optimized performance of financial-data aggregation platform
- Created bill-payment prototype integrated into financial website

Apr.–June 1999 *Embedded Systems Developer*, Green Hills Software, Santa Barbara, CA, USA.

- Ported a cross-platform linker to new targets
- Evaluated existing commonalities among embedded CPUs to simplify linker code and speed link time
- Ported C-based linker modules to C++

Feb.–Apr. 1999 *Application Software Developer*, ZBE, Goleta, CA.

- Redesigning and implementing new printer control and spooling utilities for high-performance and high-quality specialized printers

June–Sep. 1998 *SNA Server Developer/Summer Intern*, Microsoft, Redmond, WA, USA.

- Redesigned the single sign-on user management system, improving the response time as well as the recoverability of the Host Security product

1997–1998 *NT Systems Developer*, Pontis Reseach Inc., Camarillo, CA, USA.

- Specialized in distributed security in heterogeneous environments, with emphasis on Windows NT security and integration of security systems
- Tested CTOS-to-NT security interface
- Developed and tested NT NetWare Single Sign-on product
- Developed a transaction based unified NT security API with rollback capabilities

1996–1997 *Web Designer*, Student Computing Facilities, School of Environmental Science and Management, University of California at Santa Barbara, CA, USA.

- Managed the departmental network of Windows NT, Windows 95, and PowerPC computers
- Designed web pages for internal use (help pages), as well as a prototype for a database with web interface

1995–1996 *Computer-based Test Technician*, Advanced Motion Controls Camarillo, CA, USA.

- Tested the products on computer, using DAQ in-house developed software
- Improved the testing technology with regard to speed and accuracy

Personal Information

Born in Romania and naturalized citizen of the US.

Language proficiency: English, Romanian, French (written).

References

References available upon request.