Mihai Christodorescu

Department of Computer Sciences
University of Wisconsin, Madison
1210 W. Dayton St.
Madison, WI 53706, USA

Voice: +1 608-695-6271
Fax: +1 608-262-9777
http://www.cs.wisc.edu/~mihai
mihai@cs.wisc.edu

Curriculum Vitæ

Research Interests

I am interested in all aspects of computer security, with particular emphasis on software security. My current research tackles computer security problems using formal methods that combine program verification and program analysis to provide quantifiable security guarantees. My dissertation introduces techniques for the detection of malicious behavior inside obfuscated binary code.

Education

2003–present	Ph.D. in Computer Sciences, expected May 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

2001–present	*Research Assistant*, Wisconsin Safety Analyzer (WiSA) project. University of Wisconsin, Madison, WI, USA. The WiSA project focuses on the use of static analysis to detect vulnerabilities in commercial off-the-shelf components (COTS). My research work involves new approaches to the 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. The Paradyn project develops technology that aids tool and application developers in their pursuit of high-performance, scalable, parallel and distributed software. My research work produced the first reentrant binary instrumentation of running processes using the DynInst API.

Publications

Digital copies can be downloaded from http://www.cs.wisc.edu/~mihai/publications/ .

Books

1. M. Christodorescu, S. Jha, D. Maughan, D. Song, and C. Wang, editors. *Malware Detection*, volume 27 of *Advances in Information Security*. Springer-Verlag, Oct. 2006.

Publications (continued)

Conference Publications

2. M. D. Preda, M. Christodorescu, S. Jha, and S. 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)*, Nice, France, Jan. 17–19, 2007.
POPL'07 acceptance rate: 18.18% (36/198).

3. J. Giffin, M. Christodorescu, and L. 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, Dec. 5–9, 2005. Applied Computer Associates, IEEE Computer Society.
ACSAC'05 acceptance rate: 22.8% (45/197).

4. S. Rubin, M. Christodorescu, V. Ganapathy, J. T. Giffin, L. Kruger, H. Wang, and N. 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.
CCS'05 acceptance rate: 15.2% (38/250).

5. M. Christodorescu, N. Kidd, and W.-H. 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, Sept. 5–6, 2005. ACM Press.
PASTE'05 acceptance rate: 44.7% (17/38).

6. M. Christodorescu, S. Jha, S. A. Seshia, D. Song, and R. 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.
S&P'05 acceptance rate: 8.9% (17/192).

7. M. Christodorescu and S. 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.
ISSTA'04 acceptance rate: 27.9% (26/93).

8. M. Christodorescu and S. 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, Aug. 4–8, 2003. USENIX Association.
Security'03 acceptance rate: 16.4% (21/128).

Journal Publications

9. B. P. Miller, M. Christodorescu, R. Iverson, T. Kosar, A. Mirgorodskii, and F. Popovici. Playing inside the black box: Using dynamic instrumentation to create security holes. *Parallel Processing Letters*, 11(2/3):267–280, June/Sept. 2001.

Invited Publications

10. M. Christodorescu and S. Rubin. Can cooperative intrusion detectors challenge the base-rate fallacy? In *Malware Detection*, volume 27 of *Advances in Information Security*, pages 193–209, Aug. 2005. This edited volume represents the proceedings of the 2005 ARO-DHS Special Workshop on Malware Detection, Aug. 10–11, 2005, Arlington, VA, USA.

Technical Reports

11. M. Christodorescu, J. Kinder, S. Jha, S. Katzenbeisser, and H. Veith. Malware normalization. Technical Report 1539, University of Wisconsin, Madison, WI, USA, Nov. 2005.

12. J. T. Giffin, M. Christodorescu, and L. Kruger. Strengthening software self-checksumming via self-modifying code. Technical Report 1531, University of Wisconsin, Madison, WI, USA, Sept. 2005.

Publications (continued)

13. T. Kosar, M. Christodorescu, and R. Iverson. Opening pandora's box: Using binary code rewrite to bypass license checks. Technical Report 1479, University of Wisconsin, Madison, WI, USA, Apr. 2003.
14. M. Christodorescu and S. Jha. SAFE: Static analysis for executables. Technical Report 1467, University of Wisconsin, Madison, WI, USA, Feb. 2003.

Patents

15. M. Christodorescu, S. Jha, J. Kinder, S. Katzenbeisser, and H. Veith. Malware normalization. Patent application in progress, 2006.
16. M. Christodorescu and S. Jha. Method and apparatus to detect malicious software. United States patent application 20050028002, July 29, 2003.

In Submission

17. M. Christodorescu, C. Kruegel, and S. Jha. On inferring specifications of malicious behavior. In submission, Sept. 2005.

Selected Awards and Achievements

2004	Distinguished ACM SIGSOFT paper award at *International Symposium on Software Testing and Analysis (ISSTA'04)*, 2004, Boston, MA, USA. (See publication 7.)
1996–1999	Dean's honor list at University of California, Santa Barbara.

Selected Presentations

Conference Talks

May 2005	"Semantics-Aware Malware Detection" Presented at the IEEE Symposium on Security and Privacy, Oakland, CA, USA, 2005.
July 2005	"Testing Malware Detectors" Presented at the International Symposium on Software Testing and Analysis (ISSTA), Boston, MA, USA, 2004.
Aug. 2003	"Static Analysis of Executables to Detect Malicious Patterns" Presented at the 12th USENIX Security Symposium, Washington, DC, USA, 2003.

Invited Talks

Feb. 2006	"Testing Malware Detectors / Semantics-Aware Malware Detection" Presented at TrendMicro's "Meeting of the Minds," Las Vegas, NV, USA, 2006.
Sept. 2005	"Directions in Malware Detection Research" Presented at the 3rd workshop of the ARDA Malware Roadmap series, Salt Lake City, UT, USA, 2005.
Aug. 2005	"Improved Defenses through Cooperation of Network-based and Host-based Malware Detectors" Presented at the ARO–DHS Special Workshop on Malware Detection, Arlington, VA, USA, 2005.
Nov. 2003	"Static Analysis of Executables to Detect Malicious Patterns" Presented at the Software Protection Compilation Workshop, Washington, DC, USA, 2003.

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

External reviewer

Journals:	ACM Transactions on Internet Technology (TOIT): 2004. Communications of the ACM (CACM): 2005 issue on spyware. Journal of Computer Security (JCS): 2006.
Conferences:	Foundations of Computer Security Workshop (FCS): 2001. Symposium on Requirements Engineering for Info. Security (SREIS): 2002. USENIX Technical: 2004. Network and Distributed System Security Symposium (NDSS): 2005, 2007. International World Wide Web Conference (WWW): 2005. USENIX Security: 2005, 2006. International Conference on Computer Aided Verification (CAV): 2005. Software Engineering for Secure Systems (SESS): 2005. Recent Advances in Intrusion Detection (RAID): 2005. ACM Conference on Computer and Comm. Security (CCS): 2005, 2006. Workshop on Rapid Malcode (WORM): 2005. LCI International Conference on Clusters: 2006. Annual Computer Security Applications Conference (ACSAC): 2006.

Research community involvement

- 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.
- Student volunteer for the 11th USENIX Security Symposium (Security'02), Aug. 5–9, 2002, San Francisco, CA, USA.

Professional Activities (continued)

Academic activities

- 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.

Collaboration with industry

2006–present	Co-founder of Securitas Technologies, Inc., a Madison, WI, provider of behavior-based malware-detection products.
2005–present	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.

Industrial Employment

2006–present	*Principal Scientist*, Securitas Technologies, Inc., Madison, WI, USA. Spearheaded the transition of the semantics-aware malware detector from research prototype to software product.
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. Translated C-based linker modules to new C++ architecture.
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. Studied old code for reusability capabilities.
June–Sep. 1998	*SNA Server Developer/Summer Intern*, Microsoft, Redmond, WA, USA. Completely redesigned the single sign-on user management system, improving the response time as well as the recoverability of the Host Security product. Learned new technologies in a short amount of time (such as COM, DCOM, OLE, and OLEDB). Analyzed and proofed the code against threading issues, resource contention, and timing issues.
1997–1998	*NT Systems Developer*, Pontis Reseach Inc., Camarillo, CA, USA. Specialized in distributed security in heterogeneous environments, with emphasis on 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.

Industrial Employment (continued)

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. Full time employment.

Personal Information

- Born in Romania and naturalized citizen of the US.
- Language proficiency: English, Romanian, French (written).

References

References available upon request.