

# Shai Rubin

Computer Sciences Department  
University of Wisconsin-Madison  
1210, West Dayton Street  
Madison, WI 53706  
USA

Phone: +1-608-890-0019  
email: shai@cs.wisc.edu  
shai\_rubin@yahoo.com  
URL: www.cs.wisc.edu/~shai

Citizenship: Israel (J-1 Visa: has permission to work in the USA until June 2009).

## Objective

To develop new computer-security technologies in an organization that seeks novel solutions to real-world problems, emphasizes excellence, and appreciates a sincere commitment to teamwork.

## Education

**Present:** *Ph.D. candidate in Computer Science.* The University of Wisconsin-Madison (considered one of the top-ten CS departments in the U.S.). **Expected Ph.D. graduation date: July 2006.**

**1999:** *M.Sc. in Computer Science.* The Technion-Israel Institute of Technology.

**1996:** *B.A. in Computer Science (Cum laude).* The Technion-Israel Institute of Technology.

## Summary of Qualifications

- Proven ability to develop cutting-edge network security technologies.
- Improved leading network security products.
- Capable of performing independent research, prototyping, and product development.
- Demonstrated technical and scientific novelty in more than ten research papers and patents.
- Displayed leadership capabilities:
  - Lead colleagues and subordinates to accomplish goals and objectives set by management.
  - Company commander in the IDF, won the best-company award.
- Held staff-member and project-leader positions in IBM Haifa Lab.
- Demonstrated excellent communication skills while working with IBM costumers, in giving conference presentations, in writing technical reports, and in teaching.
- 10 years of combined experience in software development: C, C++, Java, Perl, Prolog, Lisp, APL, Assembly language (x86, Power), network programming.

## Experience

*Research assistant (University of Wisconsin-Madison, USA, 1999-present):*

- **Developed novel testing technology for network-based intrusion detection systems:**
  - Used the testing technology to find bugs in: Snort, TippingPoint, and Cisco IPS.
  - Worked with development teams to resolve vulnerabilities and validated fixes.
  - Worked with patent attorney and submitted a patent application describing the technology.
  - **Results:** Three papers [1,3,5]. Patent applied for by Wisconsin Alumni Research Foundation.
- **Developed methods for evaluating signatures of intrusion detection systems:**
  - Developed a novel type of signatures that describes the entire attack.
  - Implemented a “debugger” for signatures of network intrusion detection systems.
  - **Results:** A paper appeared IEEE S&P’05 [4], a highly prestigious security conference.

- **Developed anomaly-based mechanisms to detect fraud in online auctioning:**
  - Initiated a student-only project on trust in online auctioning (e.g., eBay).
  - Guided and coordinated research work among fellow students.
  - Developed statistical models to detect fraud in online auctioning.
  - **Results:** A paper appeared in CCS'05 [2]. Awarded the ACM travel grant.
  
- **Developed a language for vulnerability and risk assessment:**
  - Analyzed large network using a Nessus.
  - Proposed novel language to describe and prioritize vulnerabilities.
  - Worked with system administrator to eliminate vulnerabilities.
  - **Results:** A paper appeared in DIMVA'04 [7]. A paper selected for journal publication [6].
  
- **Developed profile-based compiler and processor optimizations:**
  - Developed profile-based compiler optimizations to improve memory locality.
  - Developed processor optimization using programming languages methods to improve instruction scheduling.
  - **Results:** Papers appeared in CC'99 [8], POPL'02 [10], and ISCA'01 [9].

*Staff-member and a project-leader (IBM Haifa Lab, Israel 1998-1999).*

- **Developed test-program generators for processor verification:**
  - Developed test program generator for DSP and VLIW architectures.
  - Worked with internal and external IBM customers.
  - Delivered software according to deadlines set by management and customers.
  - Project leader: managed and led 3 subordinates.
  - Won the Market Driven Quality Award.
  - **Results:** contribution to the verification of cutting-edge processors. A paper appeared in a ISSSP'99 [11]. Patent applied for by IBM Research. Patent granted: US patent US6567815, "Technique of clustering and compaction of binary trees".

*Company commander (Israeli Defense Forces 1990-1992).*

- Lead and managed more than one hundred soldiers and officers.
- Won the best-company award.

*Several other students/summer positions over the years in leading software companies.*

### Journal and Referred Conference Papers

1. S. Rubin, S. Jha, B. P. Miller, "On the completeness of attack mutation algorithms," In the 19th IEEE Computer Security Foundations Workshop (Venice, Italy, July 2006, to appear).
2. S. Rubin, M. Christodorescu, V. Ganapathy, J. Giffin, N. Kidd, L. Kruger, and H. Wang, "Anomaly detection as a reputation system for online auctioning," In the 12<sup>th</sup> ACM Conference on Computer and Communication Security, (Alexandria, 2005).
3. S. Rubin, S. Jha, B. P. Miller, "Using attack mutation to test a high-end NIDS," In Information Security Bulletin, Volume 10, April, 2005.
4. S. Rubin, S. Jha, B. P. Miller, "Language-based generation and evaluation of NIDS attacks," In the IEEE Symposium on Security and Privacy, (Oakland, 2005).
5. S. Rubin, S. Jha, B. P. Miller, "Automatic generation and analysis of NIDS attacks," In the Annual Computer Security Applications Conference, (Tucson, 2004).
  - Won Best Student Paper Award and
  - Best Paper Award.
6. S. Rubin, I. D. Alderman M. K. Vernon, "Foundation for intrusion prevention," In PIK –Practice in Information Processing and Communication 4(04), December, 2004.
7. S. Rubin, I. D. Alderman, D. W. Parter, M. K. Vernon, "Foundation for intrusion prevention," In Workshop on Detection of Intrusions and Malware & Vulnerability Assessment, (Germany, '04).
8. S. Rubin, R. Bodik, T. Chilimbi, "An efficient profile-analysis framework for data layout optimizations," In Proc. of the 29<sup>th</sup> Annual Symposium on Principles of Programming Languages (Portland, 2002).
9. B. A. Fields, S. Rubin, R. Bodik, "Focusing processor policies via critical-path prediction," In Proc. of the 28<sup>th</sup> Annual Intl. Symposium on Computer Architecture, (Göteborg, Sweden, 2001).
10. S. Rubin, D. Bernstein, and M. Rodeh, "Virtual cache line: A new technique to improve cache exploitation for recursive data structures," In Proc. of 8th Int. Conference on Compiler Construction, (Amsterdam, 1999).
11. S. Rubin, M. Levinger, R. Pratt, W. Moore, "Fast construction of test-program generators for digital signal processors," IEEE Conference on Acoustics, Speech, and Signal Processing, (Phoenix, 1999).

### Patents

- US patent US6567815: "Technique of clustering and compaction of binary trees".
- US patent pending "Dynamic program test generator for VLIW". Applied for by IBM.
- US patent pending "Systems and methods for testing and evaluating an intrusion detection system". Applied for by Wisconsin Alumni Research Foundation (WARF).

### Talks

<b>Date</b>	<b>Subject</b>	<b>Place</b>
11/2005	eCommerce security	ACM Conference on Computer and Communication Security, Alexandria, USA.
8/2005	Network security	CheckPoint Software Technologies, IBM Haifa lab, Intel Haifa Lab, and Rafael–Israel Armament Development Authority.
5/2005	Network security	IEEE Symposium on Security and Privacy, Oakland, CA, USA.
12/2004	Network security	Annual Computer Security Applications Conference, Tucson, USA.
8/2004	Network security	IBM Haifa Lab, Israel.
6/2004	Vulnerability assessment	Detection of Intrusions and Malware & Vulnerability Assessment, Dortmund, Deutschland.
8/2002	Program optimization	IBM Haifa Lab, Israel.
1/2002	Program optimization	29 <sup>th</sup> Annual Symposium on Principles of Programming Languages, Portland, OR, USA.
3/1999	Program optimization	8 <sup>th</sup> International Conference on Compiler Construction, Amsterdam.

### References

- **Moshe Levinger**: Manager, Simulation-Based Verification Technologies, IBM Haifa Research Lab, Israel. Phone: +972-4-829-6179, Email: [levinger@il.ibm.com](mailto:levinger@il.ibm.com)
- **Somesh Jha**: Assistant Professor, Computer Sciences Dept., University of Wisconsin-Madison, USA. Phone: +1-608-262-9519, Email: [jha@cs.wisc.edu](mailto:jha@cs.wisc.edu).
- **Barton P. Miller**: Professor, Computer Sciences Dept., University of Wisconsin-Madison, USA. Phone: +1-608-263-3378, Email: [bart@cs.wisc.edu](mailto:bart@cs.wisc.edu).
- **Ras Bodik**: Assistant Professor, Computer Science Division, University of California at Berkeley, USA. Phone: +1-510-642-2488, Email: [bodik@cs.berkeley.edu](mailto:bodik@cs.berkeley.edu).