Kevin Alejandro Roundy

roundy@cs.wisc.edu 527 E. Maple Ave.
Phone: 310-606-9692 El Segundo, CA 90245

Education

University of Wisconsin—Ph.D. in Computer Science May 2012
3.86 GPA

University of Wisconsin—Masters in Computer Science December 2005
3.86 GPA

Brigham Young University—Bachelor of Science August 2003
Major: Computer Science
Minor: Mathematics
3.78 GPA
3.87 GPA in Computer Science courses

Awards and Honors

Advanced Opportunity Fellowship 2003,2011
University of Wisconsin

1st Place Antivirus Research Grant 2011
PC Antivirus Reviews —*for study of prevalent malware obfuscations*

ORCA Scholarship/Grant 2003
Brigham Young University—*for Machine Learning research*

Undergraduate Academic Scholarship
Brigham Young University

Research Interests

My dissertation focused on building tools for *computer security* and *program analysis*. More precisely, I developed a tool to help analysts understand and control highly defensive malware programs by providing *control-* and *data-flow program analyses* and *binary instrumentation* capabilities. My tool provides the following:

- Resolution of program obfuscations and anti-tampering techniques.
- Discovery and analysis of code that is generated and/or modified at runtime, *before* the modified code executes.
- Control- and data-flow analyses of the malware program that evolve to represent changes in the program's code at runtime.
- The capacity to selectively control and monitor the malware's execution based on an up-to-date analysis of the program's code.

I achieved these goals by extending the Dyninst tool for program-binary analysis and instrumentation. Dyninst is widely used to analyze applications that do not resist analysis; I extended its code-base of 268,000 lines of C++ to handle a broad array of anti-analysis techniques. This process required changes to nearly all of Dyninst's subcomponents and gave me ample debugging and testing experience.

Other interests of mine include 0-day malware detection, virtualization-based security, and database and artificial intelligence research.

Refereed Publications

Kevin A. Roundy and Barton P. Miller. "Binary Obfuscations in Prevalent Packer Tools", *ACM Computing Surveys*, to appear.

Andrew R. Bernat, Kevin A. Roundy, and Barton P. Miller. "Efficient, Sensitivity Resistant Binary Instrumentation", *International Symposium on Software Testing and Analysis (ISSTA)*, Toronto, Canada, July 2011.

Kevin A. Roundy and Barton P. Miller. "Hybrid Analysis and Control of Malware Binaries", *Recent Advances in Intrusion Detection (RAID)*, Ottawa, Canada, September 2010.

Select Talks and Tutorials

"Analyzing Malware with Dyninst", *Wisconsin Security Research Consortium—Research Rendezvous*, Milwaukee, Wisconsin, September 2011.

"Sensitivity Resistant Analysis and Instrumentation of Malware", *Center for Computing Sciences*, Bowie, Maryland, June 2011.

"DynC Tutorial and Laboratory", *Paradyn Week*, Madison, Wisconsin, May 2011.

"Hybrid Analysis and Control of Malware Binaries", *Recent Advances in Intrusion Detection (RAID)*, Ottawa, Canada, September 2010.

"Dyninst Tutorial and Laboratory" *(in Spanish)*, *Universitat Autònoma de Barcelona (UAB)*, January 2009.

"Hybrid Analysis and Control of Malware", *Center for Computing Sciences,* Bowie, Maryland, January 2008.

Teaching Experience

I was a teaching assistant for various CS courses at the University of Wisconsin 2004-2007

Compilers	**Databases (graduate and undergraduate)**
Programming Languages	**Computer Architecture**
Data Structures	**Introduction to Programming**

In this capacity I taught study sections, designed course projects, wrote lecture notes, created test suites and scripts for evaluating projects, and set up and administered databases.

Work Experience

Symantec Research Labs May 2012—Present

Job Description: Principal Research Engineer investigating and developing practical solutions to computer security problems.

University of Wisconsin 2007—2012

Job Description: Research Assistant to Professor Barton P. Miller.

IBM Research—Almaden Summer Internship in 2005

Job Description: I extended the Java-based Xperanto tool to interpret a new query language and data model into equivalent SQL commands. This required extensive use LALR parsers (Java Cup and JFlex) and knowledge of database internals and query rewrite rules.

Brigham Young University 2002—2003

Job Description: Research Assistant to Professor Michael A. Goodrich. I applied reinforcement learning techniques to investigate the potential usefulness of touch-based warning signals sent through steering wheels and gas pedals. I adapted an open source driving simulator written in C++ to serve as an experimental platform.

Whizbang! Labs 2001—2002

Job Description: I worked extensively with information-extraction and web-crawling tools to scrape information from the web and store it as XML. I made extensive use of XPath and SQL queries, and also coded a parser (in Java) to extract content from pdf files.

Additional Programming Projects

- Co-designed an NFS-based file system server that stored files out of a PostgreSQL database. Postgres' text-indexing capabilities allowed for fast file-searching (back then, this was a novel concept).
- Designed todo-list web service in PHP that stores its data in PostgreSQL database.
- Implemented the Ethernet, CRC, ARP, IP, and TCP protocols (in C++).

Programming Skills

Languages

Extensive experience:	with C/C++, Java, x86 assembly, SQL, shell scripting
Frequent experience:	PHP, XQuery
Familiar with:	Ruby, Perl, Scheme, ML

Tools

Extensive experience:	Developing and debugging the Dyninst API's 268,000 lines of code, Use of OllyDbg, Visual Studio C++, PostgreSQL, Git, CVS
Familiar with:	Ida Pro, Ether (a Xen-based tracing tool), Intel-PIN, DB2

Platforms

Linux, Windows

Coursework

I have taken graduate level courses in: Operating Systems, Distributed Systems, Networking, Databases (2 courses), Compiler Optimizations, Programming Languages, Artificial Intelligence, Machine Learning, and Theory.

Community Service

I volunteer for the Student ACM organization and lead our department's OS reading group. I have given free tutoring services for math and computer science courses. I also coach local youth soccer leagues and offer community service through my church. I was a full-time church representative for two years in northern Italy.

Other

I speak fluent Spanish and Italian.