

Nathanael R. Paul

University of Virginia
151 Engineer's Way, P.O. Box 400740
Charlottesville, VA 22904-4740

Nationality: U.S. Citizen
<http://www.cs.virginia.edu/nate>
nate@cs.virginia.edu

- Research Interests** My research interests span many security areas including malware detection, virtual machines, and electronic voting.
- Education**
- University of Virginia, Charlottesville, VA** Aug. 2002 to Aug. 2007
Ph.D. in Computer Science
Thesis: *Disk-level Malware Detection*
Advisor: David Evans
- Clemson University, Clemson, SC** Aug. 2000 to Aug. 2002
M.S. in Computer Science
- Bob Jones University, Greenville, SC** Sept. 1997 to Aug. 2000
B.S. in Computer Science
- Research Experience**
- RESEARCH ASSISTANT Jan. 2003 to Present
University of Virginia, Charlottesville, VA
Dissertation: Disk-Level Malware Detection
For my dissertation I focused on techniques for using the disk processor to improve malware detection. Disk-level malware detection offers many advantages over past detection methods, because a disk processor: can watch all disk traffic with little overhead, can perform computation independent of the host processor, and can control any disk access before reaching the protected physical medium. We have found general rules of detection of file-infecting viruses with low false positive rates, and we have also developed a process for creating virus-specific signatures for other types of malware.
- PROJECT: Disk Drive Thermal Security**
My first work in disk drive security built on the intuition that disk drives would soon be susceptible to thermal attacks. Using a detailed thermal simulator, we showed our hypothesis of disk-level thermal vulnerabilities to be true [MSST06], and vulnerable disk drives are now available commercially.
- PROJECT: Virtual Machine Security**
I studied virtual machines by examining the low-level bytecode verifier that all the other virtual machine security guarantees rely on. This work showed how Microsoft .NET's virtual machine design was able to avoid past mistakes of the Java virtual machine. None of the low-level bytecode verification security vulnerabilities were present in the Microsoft .NET virtual machine, and we attributed this to the different bytecode verifier designs [ACSAC04, CS06].
- PROJECT: Cryptanalysis of Instruction Set Randomization**
We developed an attack on a specially protected server where each address of memory used to store the code of a program is encrypted with some secret key. This defense makes many memory-based attacks useless, because the addresses on the stack are encrypted. While our attack required a lot of overhead, we were able to break the keys used to protect the memory. To make this attack feasible in spreading rapidly, I developed a micro-virtual machine that required less than 100 bytes of keys [USENIX05].
- PROJECT: Electronic Voting**
Inspired by D. Chaum's earlier work on electronic voting, I explored voter authentication using one-time pads that a voter can verify visually [HCI03]. This provides a workable verification solution that can be used to authenticate voters even when their PCs cannot be trusted. We also studied the voter's perception of security versus the actual security provided by different voting methods [IEEEESP04].

	RESEARCH ASSISTANT	Jan. 2001 to Aug. 2002
	Clemson University, Clemson, SC	
	I designed and developed tools for a project management tool using role-based access control.	
Teaching Experience	TUTOR	Fall 2006
	CS 110: Introduction to Information Technology	
	MDST 110: Information Technology and Digital Media	
	University of Virginia, Charlottesville, VA	
	During the fall semester I helped tutor UVa athletes in different courses (primarily CS 110 and MDST 110).	
	RESEARCH MENTOR	Summer 2007
	I mentored an undergraduate in researching the performance aspects of disk-level malware detection, and I helped another graduate student work on automating the process for creating behavior-specific signatures.	
	RESEARCH MENTOR	Summer 2006
	During the past summer, I guided an undergraduate in researching disk-level malware detection. She was a finalist in the Fall 2006 UVa Undergraduate Research Symposium, and she presented a work-in-progress talk on this work at USENIX Security in August 2006.	
	COURSE CO-COORDINATOR	Spring 2004
	CS 851: Malware Seminar	
	Other Co-coordinators: David Evans, Anh Nguyen-Tuong	
	University of Virginia, Charlottesville, VA	
	As a seminar course, graduate students interested in malware proposed research projects to work on during the semester. My responsibilities included helping to create a course outline by finding interesting papers for weekly discussion, reviewing project proposals, and providing helpful comments to the students in malware research. Our ideas for our USENIX 2005 paper on instruction set randomization originated in this seminar.	
	TEACHING ASSISTANT	Aug. 2002 to Dec. 2002
	CS 551/651: Information Assurance	
	Instructor: Anita Jones	
	University of Virginia, Charlottesville, VA	
	This was an undergraduate/graduate security and cryptography course. I helped design and grade both homework and exams.	
	TEACHING ASSISTANT	Aug. 2000 to Dec. 2000
	CPSC 111: Elementary Computer Programming in C/C++	
	Instructor: Rose M. Lowe	
	Clemson University, Clemson, SC	
	This course was an introductory undergraduate C++ course that I designed and taught labs for ~20 students.	
Other Experience	CONSULTANT	Aug. 2006 to Present
	Alltec Services, Carbondale, CO	
	I answer any technical questions that arise in this burglar and fire alarm company including topics on security cameras and networking.	
	JR. SYSTEMS ADMINISTRATOR	Summer/Christmas 2000
	Milliken & Co., Marietta, SC	
	I developed applications to analyze performance of dye machines. I also performed systems administration duties including installing a radio frequency identification system, maintaining network printers, and troubleshooting general network problems in the system administrator's absence.	

In Submission	Nathanael Paul, Adrienne Felt, Sudhanva Gurumurthi, and David Evans. Disk-level Behavioral Virus Detection.
Publications	<p>[CS06] Nathanael Paul and David Evans. Comparing Java and .NET Security: Lessons Learned and Missed. In <i>Computers & Security</i>, Volume 25, Issue 5, July 2006. (Expanded version of [ACSAC04])</p> <p>[MSST06] Nathanael Paul, Sudhanva Gurumurthi, and David Evans. Thermal Attacks on Storage Systems. In the <i>Proceedings of the NASA/IEEE Conference on Mass Storage Systems and Technologies (MSST)</i>, May 2006.</p> <p>[COBASSA05] Nathanael Paul, Sudhanva Gurumurthi, and David Evans. Towards Disk-level Malware Detection. In <i>Workshop on Code Based Software Security Assessments.(CoBaSSA)</i>, November 2005.</p> <p>[USENIX05] Nora Sovarel, David Evans, and Nathanael Paul. Where's the FEEB? The Effectiveness of Instruction Set Randomization. In the <i>Proceedings of the 14th USENIX Security Symposium</i>, August 2005.</p> <p>[ACSAC04] Nathanael Paul and David Evans. .NET Security: Lessons Learned and Missed from Java. In the <i>Proceedings of the 20th Annual Computer Security Applications Conference (ACSAC)</i>, December 2004. (Expanded version published as [CS06])</p> <p>[IEEEESP04] David Evans and Nathanael Paul. Election Security: Perception and Reality. <i>IEEE Security and Privacy</i>, January/February 2004.</p> <p>[HCI03] Nathanael Paul, David Evans, Avi Rubin, and Dan Wallach. Authentication for Remote Voting. In <i>Workshop on Human-Computer Interaction and Security Systems</i>, April 2003.</p>
Grants/ Proposals	<p>SENIOR PERSONNEL</p> <p>Disk-level Malware Detection and Response. NSF Cybertrust Award (\$400,000). August 2006. I contributed the technical content for the proposal which is based on my PhD proposal.</p>
Patents	Method, System and Computer Program Product for Behavioral Malware Detection Analysis, and Response. Nathanael Paul, David Evans, Sudhanva Gurumurthi, and Adrienne Felt. U.S. Patent 60/852,609 (<i>Provisional Patent</i>).
Scholarships/ Fellowships	<p>Life Scholarship, Bob Jones University (1998-2000)</p> <p>Dean's Fellow, University of Virginia (2002-2005)</p> <p>Renewed for maximum of 3 years.</p>