Nikhil Swamy

Department of Computer Science
University of Maryland
College Park, MD 20742

Email: nswamy@cs.umd.edu
Web: www.cs.umd.edu/∼nswamy
Tel: +1 202 431 3472

Research Interests

My research is focused primarily on improving the security, reliability and performance of software systems by utilizing formal methods in the design, implementation or analysis of programming languages.

Education

University of Maryland at College Park, College Park, MD

- Ph.D. in Computer Science; expected Summer '08
  Dissertation: *A Language-based Approach to Web-application Security*
- M.S. in Computer Science; May 2005

Hampshire College, Amherst, MA

- B.A. (Majors: Computer Science, Mathematics); May 2000
  Thesis: *Automated Reasoning about Abstract Algebra: Control Strategies for Supported Deductions*

Research Projects

As a research assistant at the University of Maryland under the guidance of Dr. Michael Hicks, I have worked on several projects. Some of these are summarized below.

Language-based Approaches to Web-Application Security
My dissertation work explores the usage of various forms of lightweight dependent-typing to provably enforce practical security policies in software. To this end, I have designed and implemented a novel type system for the Links web programming language in which a wide range of security policies, wider than in any other single language, are provably enforceable. With the assistance of another student, I have implemented two relatively large applications using my enhancements to Links, demonstrating that complex, realistic policies can be enforced end-to-end, across the multiple tiers of a web-application. These are some of the very first applications ever constructed in a security-typed programming language.

Defeating Cross-site Scripting Attacks
Cross-site scripting attacks were listed in as the most common class of security vulnerability in 2007 by Mitre. I co-designed and implemented BEEP, an extension to the JavaScript interpreters in a number of common browsers that can be used by web site designers to guarantee that clients that visit their web sites are protected against such attacks. We showed that with some simple tool support, a web site can easily be retrofitted with BEEP controls while incurring only a small performance penalty.

Dynamic Policy Updates in a Security-Typed Language
The security privileges of the principals that interact with real systems typically change over time. However, security-typed languages have generally required security policies to remain fixed statically. As part of my effort to make these languages more practical, I designed a language that allows information flow policies to be provably enforced even though the policy is allowed to change at runtime.

The Cyclone Programming Language
Cyclone aims to bring the benefits of type safety to low-level systems software like OS device drivers. I co-designed and implemented a framework of pointer qualifiers and a modular whole-program analysis that allows certain qualifiers annotations to be inferred. I used my qualifier extensions to port several Linux device drivers to Cyclone, proving the safety of pointer arithmetic and the explicit deallocation of individual objects. My contributions are part of Cyclone-1.0, the first major release, and I remain one of the principal maintainers of Cyclone.

Professional Experience

Microsoft Research *Summer Intern*
Cambridge, UK **May 2006 – July 2006** and **April 2007**
My work during this internship involved analyzing implementations of multi-party cryptographic protocols in the web services modules of Windows Vista. We used a novel technique to compile F# programs to processes in the scripting language of the ProVerif automated theorem prover. Our main results included automated proofs for the largest implementations of cryptographic protocols to date.

IBM T.J. Watson Research Center *Summer Intern*
Hawthorne, NY. **May 2004 – August 2004**
I worked with the Jikes VM team on investigating multi-lingual support in a virtual machine. Our approach involved designing novel abstractions for the JIT compiler and GC to be able to support cross-language calls.

IBM T.J. Watson Research Center *Summer Intern*
Hawthorne, NY. **May 2003 – August 2003**
I worked with the e-business tools group to analyze and optimize the security enforcement components of the WebSphere application server. I helped develop a tool to recover context-sensitive profiling information from detailed logs generated by a performance monitor. We used this tool to optimize away many redundant checks in the enforcement of Java's stack inspection policy.

Corporate Technologies, Inc. *Software Engineer*
Burlington, MA. **June 2000 – June 2002**
I consulted as an applications engineer for various clients in the field of operations research. Much of my work involved constructing J2EE applications that streamlined the management of business-to-business supply chains.

Teaching

Guest lecturer

CMSC 631 : Program Analysis and Understanding	Fall 2007

Teaching assistant

CMSC 330 : Organization of Programming Languages	Fall 2005
CMSC 351 : Algorithms	Spring 2004
CMSC 351 : Algorithms	Fall 2003
CMSC 351 : Algorithms	Spring 2003
CMSC 330 : Organization of Programming Languages	Fall 2002

Publications

Conference and selective workshop papers

1. **Fable: A Language for Enforcing User-defined Security Policies**
   Nikhil Swamy, Brian J. Corcoran and Michael Hicks
   In Proceedings of the 29th IEEE Symposium on Security and Privacy (S&P); Oakland, California; May 2008 (To appear). Acceptance rate 28/249 (11%).
2. **Verified Implementations of the Information Card Federated Identity Management Protocol**
   Karthikeyan Bhargavan, Cédric Fournet, Andrew D. Gordon and Nikhil Swamy
   In Proceedings of the 3rd ACM Symposium on Information, Computer and Communication Security (ASIACCS); Tokyo, Japan; March 2008 (To appear). Acceptance rate 41/182 (22%).

3. **Verified Enforcement of Security Policies for Cross-Domain Information Flows**
   Nikhil Swamy, Michael Hicks, and Simon Tsang
   In Proceedings of the 2007 Military Communications Conference (MILCOM); Orlando, Florida; October 2007.
4. **Defeating Script Injection Attacks with Browser Enforced Embedded Policies**
   Trevor Jim, Nikhil Swamy, and Michael Hicks
   Proceedings of the 16th International World Wide Web Conference (WWW); Banff, Canada; May 2007. Acceptance rate 10/63 (16%) for the security track, 111/740 (15%) overall.
5. **Managing Policy Updates in Security-typed Languages**
   Nikhil Swamy, Michael Hicks, Stephen Tse, and Steve Zdancewic
   Proceedings of 19th IEEE Computer Security Foundations Workshop(CSFW); Venice, Italy; July 2006. Acceptance rate 25/96 (26%). Note: though termed a workshop, based on citation rate and number of submissions, CSFW has effectively been a conference for many years; as of 2007, CSFW has been renamed CSF and is termed a symposium.
6. **Finding and Removing Performance Bottlenecks in Large Systems**
   Glen Ammons, Jong-Deok Choi, Manish Gupta, and Nikhil Swamy
   In Proceedings of The European Conference of Object-oriented Programming (ECOOP); Oslo, Norway; May 2004. Acceptance rate 25/132 (19%).
7. **Finding a Better-than-classical Quantum AND/OR Algorithm**
   Lee Spector, Howard Barnum, Herbert J. Bernstein, and Nikhil Swamy
   In Proceedings of the 1st IEEE Congress of Evolutionary Computation (CEC); Washington, DC; July 1999.

Working papers

Verified Enforcement of Automaton-based Information Release Policies
Nikhil Swamy and Michael Hicks
In submission. Available at www.cs.umd.edu/∼nswamy/papers/lair.pdf

Journal articles and book chapters

1. **Safe Manual Memory Management in Cyclone**
   Nikhil Swamy, Michael Hicks, Greg Morrisett, Dan Grossman, and Trevor Jim
   Science of Computer Programming (SCP), 62(2), Special Issue on Memory Management; October 2006.
2. **Dynamic Inference of Polymorphic Lock Types**
   James Rose, Nikhil Swamy, and Michael Hicks
   Science of Computer Programming (SCP), 58(3), Special Issue on Concurrency and Synchronization in Java Programs; December 2005.
3. **Applying Genetic Programming to Quantum Computation**
   Lee Spector, Howard Barnum, Herbert J. Bernstein, and Nikhil Swamy
   Book Chapter in Advances in Genetic Programming III; L.Spector et al. ed.; MIT Press, 1999.

Workshop papers

1. **Combining Provenance and Security Policies in a Web-based Document Management System (Extended abstract)**
   Brian Corcoran, Nikhil Swamy, and Michael Hicks.
   In On-line Proceedings of the Workshop on Principles of Provenance (PrOPr); Edinburgh, Scotland; November 2007.

2. **Dynamic Inference of Polymorphic Lock Types**
   James Rose, Nikhil Swamy, and Michael Hicks
   In Proceedings of the ACM Conference on Principles of Distributed Computing (PODC) Workshop on Concurrency and Synchronization in Java Programs (CSJP); Newfoundland, Canada; July 2004.
   Acceptance rate 11/24 (46%).
3. **RGL : A Study in a Hybrid Real-time System**
   Ken Hennacy, Nikhil Swamy, and Don Perlis
   In Proceedings of Neural Networks and Computational Intelligence (NCI); Cancun, Mexico; May 2003.

Technical reports

1. **Fable: A Language for Enforcing User-defined Security Policies**
   Nikhil Swamy and Michael Hicks
   Department of Computer Science, University of Maryland, Technical Report CS-TR-4876; July 2007.
2. **Toward Specifying and Validating Cross-Domain Policies**
   Michael Hicks, Nikhil Swamy, and Simon Tsang
   Department of Computer Science, University of Maryland, Technical Report CS-TR-4870; April 2007.
3. **Defeating Script Injection Attacks with Browser-Enforced Embedded Policies**
   Trevor Jim, Nikhil Swamy, and Michael Hicks.
   Department of Computer Science, University of Maryland, Technical Report CS-TR-4835; November 2006.
4. **Managing Policy Updates in Security-Typed Languages (Extended Version)**
   Nikhil Swamy, Michael Hicks, Stephen Tse and Steve Zdancewic
   Department of Computer Science, University of Maryland; Technical Report CS-TR-4793; June 2006.
5. **A Distributed Algorithm for Constructing a Generalization of de Bruijn Graphs**
   Nikhil Swamy and Konstantinos Bitsakos and Nikolaos Frangiadakis
   Department of Computer Science, University of Maryland, Technical Report CS-TR-4792; June 2006.

Invited Talks and Posters

1. **End-to-End Security of Cross-Domain Information Flows**
   Invited talk and poster at U.S. Army Research Laboratory's Collaborative Technology Alliance Program; Fort Monmouth, New Jersey; November 2007.
2. **Managing Policy Updates in Security-Typed Languages**
   • Invited talk at the School of Informatics, University of Edinburgh; April 2007.
   • Poster and short talk for Security and Privacy Day at IBM T.J. Watson Research Center, New York; November 2006.

Service

Journal reviewing: ACM Transactions on Software Engineering (TSE)
External journal reviewing: Science of Computer Programming (SCP)
External conference reviewing: ECOOP '08, OOPSLA '07, PLDI '07, COORDINATION '07, PLAS '07
Member of the Department of Computer Science Student's Executive Council : 2004-2007
Incoming student mentorship : 2005, 2007

References

Michael Hicks
Assistant Professor
Department of Computer Science
University of Maryland, College Park
College Park, MD 20742
Tel:+1-301-405-2710
Email: mwh@cs.umd.edu

Jeffrey Foster
Assistant Professor
Department of Computer Science
University of Maryland, College Park
College Park, MD 20742
Tel: +1-301-405-2751
Email: jfoster@cs.umd.edu

Greg Morrisett
Allen B. Cutting Professor of Computer Science
School of Engineering and Applied Sciences
Harvard University
Cambridge, MA 02138
Phone: +1-617-495-9526
Email: greg@eecs.harvard.edu

Trevor Jim
AT&T Labs Research
180 Park Avenue
P.O. Box 971
Florham Park, NJ 07932
trevor@research.att.com

Karthikeyan Bhargavan
Mircosoft Research Cambridge
7 J.J. Thomson Avenue
Cambridge, CB3 0FB
United Kingdom
karthb@microsoft.com