

VIVEK HALDAR
vhaldar@uci.edu
http://www.ics.uci.edu/~vhaldar

Room 105, CSE
Information and Computer Science,
University of California,
Irvine, CA 92697

OBJECTIVE: Research and development position in trusted computing, virtual machines and language-based security.

EDUCATION

- 2002 - PhD candidate, Information and Computer Science, University of California, Irvine.
(Expected graduation: Winter 2006)
- 2000 – 2002 Master of Science, Information and Computer Science, University of California, Irvine.
- 1996 – 2000 Bachelor of Technology, Computer Science, Indian Institute of Technology, New Delhi.

WORK EXPERIENCE

- June - Sept 2004 Internship at Sun Microsystems Laboratories, Mountain View, CA.
Added licensing and DRM components to the Java Self-Organizing Media project.
- June - Sept 2002 Internship at Sun Microsystems Laboratories, Mountain View, CA.
Worked on verifiable performance-enhancing annotations for Java bytecode.

RESEARCH INTERESTS

Trusted computing, language-based security, virtual machines, mobile code representations, compilers

RESEARCH OVERVIEW

Trusted Computing and Semantic Remote Attestation: Remote attestation is one of the core functionalities provided by trusted computing platforms. It holds the promise of enabling a variety of novel applications. However, current techniques for remote attestation are static, inexpressive and fundamentally incompatible with today's heterogeneous distributed computing environments and commodity open systems. Using language-based virtual machines enables the remote attestation of complex, dynamic, and high-level program properties – in a platform-independent way. We call this *semantic remote attestation*.

This enables a number of novel applications that distribute trust dynamically. I am currently designing and implementing a framework for semantic remote attestation built on the Java Virtual Machine, as well as example applications to run on it. Among the properties we attest are: dynamic information flow using mandatory access control at the object level in the JVM, which allows the specification and enforcement of fine-grained policies based on tracking data items throughout the execution of a program; and taint propagation information for securing web applications.

Verifiable Annotations for reducing just-in-time compilation overhead: Annotations are often added to mobile code to reduce the optimization burden of just-in-time compilers. However, these annotations are not checked for correctness and must be trusted – incorrect or malicious annotations could lead to the generation of incorrect or insecure code. I have worked on time- and space-efficient methods for verifying the results of the large class of data flow optimizations, as well as virtual machine architectures that are designed to use them. This allows the safe movement of computation-intensive optimizations away from the code consumer towards the code producer. (Some of this work was done at Sun Labs during a summer internship in 2002.)

Novel mobile code representations: Mobile code formats based on bytecode are the norm, but they suffer from the disadvantages of being hard to optimize and hard to prove safe, due to the large semantic gap between bytecode and source languages. Using abstract syntax trees (ASTs) as a mobile code format has numerous advantages over bytecode formats. ASTs are portable, inherently safer, easier to optimize, and much more compact than bytecode. I have helped design and develop a framework for using ASTs as a mobile code format, which we have used for Java source programs.

SELECTED PUBLICATIONS

PEER REVIEWED CONFERENCES AND WORKSHOPS

Dynamic Taint Propagation for Java; Vivek Haldar, Deepak Chandra and Michael Franz; to appear in the Annual Computer Security Applications Conference (ACSAC), December 2005.

Practical, Dynamic Information Flow for Virtual Machines; Vivek Haldar, Deepak Chandra and Michael Franz; Workshop on Programming Language Interference and Dependence, September 2005.

Symmetric Behavior-Based Trust: A New Paradigm for Internet Computing; Vivek Haldar and Michael Franz; New Security Paradigms Workshop, September 2004 (Also selected for a panel discussion at the Applied Computer Security Associates Conference, December 2004).

Semantic Remote attestation: A Virtual Machine Directed Approach to Trusted Computing; Vivek Haldar, Deepak Chandra, and Michael Franz; USENIX Virtual Machine Research and Technology Symposium (USENIX VM), May 2004 (Awarded **Best Paper**)

Making Mobile Code Both Safe And Efficient; M. Franz, W. Amme, M. Beers, N. Dalton, P. H. Froehlich, V. Haldar, A. Hartmann, P. S. Housel, F. Reig, J. von Ronne, Ch. H. Stork, and S. Zhenochin; in J. Lala (Ed.), Foundations of Intrusion Tolerant Systems; IEEE Computer Society Press; January 2004

A Portable Virtual Machine Target for Proof-Carrying Code; Michael Franz, Deepak Chandra, Andreas Gal, Vivek Haldar, Fermin Reig and Ning Wang; ACM SIGPLAN 2003 Workshop on Interpreters, Virtual Machines and Emulators (IVME), June 2003

The Source is the Proof; Vivek Haldar, Christian H. Stork and Michael Franz; New Security Paradigms Workshop, September 2002 (Also selected for a panel discussion at the Applied Computer Security Associates Conference, December 2002).

Towards Trusted Systems from the Ground Up; Vivek Haldar and Michael Franz; in the proceedings of the Tenth ACM SIGOPS European Workshop, September 2002

Towards Language-Agnostic Mobile Code; Christian H. Stork, Peter Housel, Vivek Haldar, Niall Dalton and Michael Franz; First Workshop on Multi-Language Infrastructure and Interoperability, September 2001, Firenze, Italy

Compressed Abstract Syntax Trees for Mobile Code; Christian H. Stork and Vivek Haldar; Workshop on Intermediate Representation Engineering (IRE 2001), July 2001, Orlando, Florida

TECHNICAL REPORTS

Virtual Machine Driven Dynamic Voltage Scaling; Vivek Haldar, Ch. W. Probst, V. Venkatachalam, and M. Franz; Technical Report No. 03-21, School of Information and Computer Science, University of California, Irvine; October 2003

Verifying Data Flow Optimizations for Just-in-Time Compilation; Vivek Haldar; Sun Labs Technical Report 2002-118, October 2002

Online Verification of Offline Escape Analysis; Michael Franz, Vivek Haldar, Chandra Krintz, Christian H. Stork; Technical Report No. 02-21, Department of Information and Computer Science, University of California, Irvine; September 2002