Dr. Amit Vasudevan

Contact Information

Research Systems Scientist
CyLab, Carnegie Mellon University

E-mail: amitvasudevan@acm.org
amitvasudevan@hypcode.org
WWW: http://hypcode.org

Research Interests

- Trusted Computing, Formal Verification and Virtualization Security
  - Secure hypervisors and hypervisor verification methodologies
  - Trustworthy execution and execution provenance/logging
- Security of mobile devices including mobile phones, laptops and tablets
- Malware (malicious-code) analysis and detection
- Operating system security and kernel architecture

Teaching Interests

Computer Architecture and Assembly Language Programming, C Programming, Systems Programming, Virtualization/Hypervisors, Trusted Computing, Malware Analysis, Operating Systems, Embedded Systems

Education

The University of Texas, Arlington, Arlington, TX, USA

Ph.D., Computer Science and Engineering, May 2007

- Thesis title: *WiLDCAT: An Integrated Stealth Environment for Dynamic Malware Analysis*
- Advisor: Prof. Ramesh Yerraballi
- GPA: 4.0/4.0

M.S., Computer Science and Engineering, December 2003

- Thesis title: *Sakthi: A Retargetable Dynamic Framework for Binary-Instrumentation*
- Advisor: Prof. Ramesh Yerraballi
- GPA: 4.0/4.0

BMS College of Engineering (Bangalore University), Bangalore, India

B.E., Computer Science and Enginering, September 2001

- GPA: First Class with Distinction, 3.9/4.0

Academic Appointments

Carnegie Mellon University

Research Systems Scientist **October 2010 to present**
CyLab

Responsibilities include basic research in the field of computer security with an emphasis on trustworthy computing, formal verification, virtualization security and embedded/mobile virtualization; software development, and solicitation of research funding. Active research projects:

- eXtensible, Modular Hypervisor Framework (XMHF)
- Hypervisor Verification
- Hypervisor-based Verifiable Platform Resource Accounting
- Isolated Execution on Mobile Devices
- On-CPU Isolation and Root-of-Trust

Active open-source software development:

- `xmhf.org`. An extensible, modular and formally verifiable hypervisor framework for x86 systems (AMD/Intel) with support for dynamic root of trust, hypervisor boot integrity measurement and isolated execution for security-sensitive code.
- `uberspark.org`. A formally-backed (system) software verification framework enforcing verifiable object abstractions for automated compositional verification of security properties.

Carnegie Mellon University

Postdoctoral Researcher **September 2007 to October 2010**

CyLab

Responsibilities include research in virtualization security, malware analysis and trustworthy computing; software development, and solicitation of research funding. Research projects include:

- Lockdown: Towards a Safe and Practical Architecture for Security Applications
- Secure Execution Trace Recording
- SecVisor: Kernel-mode Execution Integrity
- Tracking Unknown (0-day) Malware

The University of Texas at Arlington

Assistant Instructor **January 2004 to May 2007**

Department of Computer Science and Engineering

Taught undergraduates CSE2312: Computer Organization and Assembly Language Programming and CSE1301: Introduction to C Programming. Set course syllabus, authored and delivered course lectures, designed exams and assignments.

Professional Experience

NoFuss Security, Inc, Pittsburgh, PA, USA

Senior Security Architect **February 2011 to 2013**

Member of three-person engineering team: design, development, and support for commercialization of trustworthy computing technologies. Principal investigator on a project on analysis of COTS hypervisor security. Major tasks included systematic attack surface enumeration, discovery of design-level vulnerabilities and constructing mitigation approaches.

Cognizant Technologies and Solutions Corp., India

Programmer Analyst **January 2002 to May 2002**

Developed a bridge framework (native C to Enterprise Java Beans) for faster porting of existing native Solaris/C application containers to Enterprise Java Beans.

Bharat Electronics, India

Research Intern **June 2001 to December 2001**

Designed software control mechanisms and a command and control center for monitoring and controlling a group of remote naval radar units.

Books and Book Chapters

[1] Amit Vasudevan. "Security Properties for Commodity Platforms: Verifiable Micro-Hypervisor Framework". Springer Briefs in Computer Science, 2018. **(Invited; In Preparation)**

[2] Amit Vasudevan, Jonathan M. McCune, James Newsome. "Trustworthy execution on mobile devices. What security properties can my mobile platform give *me*?". Springer Briefs in Computer Science. Springer, ISBN 978-1-4614-8189-8, 2014. **(Invited)**

[3] Amit Vasudevan. "Effective Malware Analysis Using Stealth Breakpoints". In Strategic and Practical Approaches for Information Security Governance: Technologies and Applied Solutions. IGI Global, ISBN-10: 1466601973, 2012 **(Invited)**

Refereed Publications

[4] Amit Vasudevan, Sagar Chaki, Petros Maniatis, Limin Jua, Anupam Datta. "UberSpark: Enforcing Verifiable Object Abstractions for Automated Compositional Security Analysis of a Hypervisor". In USENIX Security Symposium 2016.

[5] Emmanuel Owusu, Jorge Guajardo, Jonathan M. McCune, James Newsome, Adrian Perrig, Amit Vasudevan. "OASIS: on achieving a sanctuary for integrity and secrecy on untrusted platforms". In ACM Conference on Computer and Communications Security 2013.

[6] Amit Vasudevan, Sagar Chaki, Limin Jia, Jonathan McCune, Jim Newsome, Anupam Datta. "Design, Implementation and Verification of an eXtensible and Modular Hypervisor Framework". In IEEE Symposium on Security and Privacy, 2013.

[7] Chen Chen, Petros Maniatis, Adrian Perrig, Amit Vasudevan, Vyas Sekar. "Towards Verifiable Resource Accounting for Outsourced Computation". In ACM Virtual Execution Environments, 2013.

[8] Carsten Willems, Ralf Hund, Amit Vasudevan, Andreas Fobian, Dennis Felsch, Thorsten Holz. "Down to the Bare Metal: Using Processor Features for Binary Analysis". In IEEE Annual Computer Security and Applications Conference (ACSAC), 2012.

[9] Amit Vasudevan, Bryan Parno, Ning Qu, Virgil D. Gligor, Adrian Perrig. "Lockdown: Towards a Safe and Practical Architecture for Security Applications on Commodity Platforms". In International Conference on Trust and Trustworthy Computing (TRUST), Vienna, Austria, 2012.

[10] Amit Vasudevan, Emmanuel Owusu, Zongwei Zhou, James Newsome, Jonathan M. McCune. "Trustworthy Execution on Mobile Devices: What Security Properties Can My Mobile Platform Give Me?". In International Conference on Trust and Trustworthy Computing (TRUST), Vienna, Austria, 2012.

[11] Amit Vasudevan, Jonathan McCune, James Newsome, Adrian Perrig, Leendert van Doorn. "CARMA: A Hardware Tamper-Resistant Isolated Execution Environment on Commodity x86 Platforms". In ACM Symposium on Information, Computer and Communications Security (ASIACCS), 2012.

[12] Jason Franklin, Sagar Chaki, Anupam Datta, Jonathan M. McCune, Amit Vasudevan. "Parametric Verification of Address Space Separation". In First Conference on Principles of Security and Trust (POST) 2012. **(Best Paper Nomination)**

[13] Amit Vasudevan, Ning Qu and Adrian Perrig, "XTRec: Secure Real-time Execution Trace Recording on Commodity Platforms". In 44th Hawaii International Conference in System Sciences (HICSS), Hawaii, 2011. **(Best Paper Nomination)**

[14] Amit Vasudevan, Jonathan M. McCune, Ning Qu, Leendert van Doorn and Adrian Perrig, "Requirements for an Integrity-Protected Hypervisor on the x86 Hardware Virtualized Architecture". In 3rd International Conference on Trust and Trustworthy Computing (TRUST), Berlin, Germany, 2010.

[15] Amit Vasudevan, "Reinforced Stealth Breakpoints". In 4th IEEE Conference on Risks in Internet Systems (CRiSIS), Toulouse, France, 2009.

[16] Amit Vasudevan, "MalTRAK: Tracking and Eliminating Unknown Malware". In IEEE 24st Annual Computer Security and Applications Conference (ACSAC), Anaheim, CA, 2008.

[17] Amit Vasudevan and Ramesh Yerraballi, "Cobra: Fine-grained Malware Analysis using Stealth Localized-executions". In 2006 IEEE Symposium on Security and Privacy, Oakland, CA.

[18] Amit Vasudevan and Ramesh Yerraballi, "SPiKE: Engineering Malware Analysis Tools using Unobtrusive Binary-Instrumentation". In 29th Australasian Conference in Computer Science (ACSC), Hobart, Australia, 2006. **(Best Paper Nomination)**

[19] Amit Vasudevan and Ramesh Yerraballi, "Stealth Breakpoints". In IEEE 21st Annual Computer Security and Applications Conference (ACSAC), Tucson, AZ, 2005.

[20] Ashish Chawla, Ramesh Yerraballi and Amit Vasudevan, "Coalesced QoS: A Pragmatic Approach to a Unified Model to Support Quality Of Service (QoS) in High Performance Kernel-Less Operating System (KLOS)". In Advances in Systems, Computing Sciences and Software Engineering: Proceedings of SCSS 2005 (14), December 2005. ISBN-10: 1-4020-5262-6.

[21] Amit Vasudevan, Ramesh Yerraballi and Ashish Chawla, "A High Performance Kernel-Less Operating System Architecture". In 28th Australasian Conference in Computer Science (ACSC), New Castle, Australia, 2005.

[22] Amit Vasudevan and Ramesh Yerraballi, "SAKTHI A Retargetable Dynamic Framework for Binary Instrumentation". In 2004 Hawaii International Conference on Computer Sciences (HICCS), Honolulu, HI, 2004. ISSN:1545-672.

[23] Amit Vasudevan, Ramesh Yerraballi and Ashish Chawla, "KLOS A High Performance Kernel-Less Operating System". In 2003 IEEE RTSS Work in Progress.

Technical Reports

[24] Amit Vasudevan, Sagar Chaki, Petros Maniatis, Limin Jia, and Anupam Datta. "UberSpark: Enforcing Verifiable Object Abstractions for Automated Compositional Security Analysis of a Hypervisor". CMU CyLab Technical Report CMU-CyLab-16-003. June 2016.

[25] Sagar Chaki, Amit Vasudevan, Limin Jia, Jonathan M. McCune, and Anupam Datta. "Design, Development and Automated Verification of an Integrity-Protected Hypervisor". CMU CyLab Technical Report CMU-CyLab-12-017. July 2012.

[26] Amit Vasudevan, Jonathan M. McCune, and James Newsome. "Design and Implementation of an eXtensible and Modular Hypervisor Framework". CMU CyLab Technical Report CMU-CyLab-12-014. June 2012.

[27] Jason Franklin, Sagar Chaki, Anupam Datta, Jonathan Mccune and Amit Vasudevan. "Parametric Verification of Address Space Separation". CMU Cylab Technical Report CMU-CyLab-12-001. January 2012.

[28] Amit Vasudevan, Emmanuel Owusu, Zongwei Zhou, James Newsome, and Jonathan McCune. "Trustworthy Execution on Mobile Devices: What security properties can my mobile platform give me?". CMU CyLab Technical Report CMU-CyLab-11-023. November 2011.

[29] Amit Vasudevan, Bryan Parno, Ning Qu and Adrian Perrig. "Lockdown: A Safe and Practical Environment for Security Applications". CMU CyLab Technical Report CMU-CyLab-09-011. July 2009.

[30] Amit Vasudevan, Ning Qu, Adrian Perrig. "XTREC: Secure Realtime Instruction-level Control Flow Recording on Commodity Platforms". CMU CyLab Technical Report CMU-CyLab-09-007. March 2009.

Patents

[1] Number 2014/0258736 A1. Inventor(s): Jorge G. Merchan, Emmanual K. Owusu, Jonathan M. McCune, James D. Newsome, Amit Vasudevan, Adrian Perrig (equal rights). "Systems and Methods for Maintaining Integrity and Secrecy in Untrusted Computing Platforms", Date: 11/2014.

[2] Number 61/273,454. Inventor(s): Virgil D. Gligor, Adrian Perrig, Anupam Datta, Jonathan M. McCune, Ning Qu, Bryan J. Parno, Amit Vasudevan, Yanlin Li (equal rights). "User-Verifiable Execution of Security-Sensitive Code on Untrusted Platforms", Date: 04/2009.

Grants

[1] "Verified and Verifiable Security Properties on Untrusted Computing Platforms", Intel Corp., 2013-2014. [Role: Co-PI, $150,000]

[2] "COTS Hypervisor Security: Architectural Analysis", United States Air Force, 2011. [Role: PI, $50,000]

[3] "Real-time Execution Trace Recording and Analysis on Commodity Platforms", Northrup Grumman, 2009-2010. [Role: Co-PI, $200,000]

[4] "Hypervisor-based Secure Virtualization", United States Air Force, 2008-2009. [Role: Lead Researcher, $170,000]

Teaching Experience

The University of Texas at Arlington, Arlington, TX

Assistant Instructor **January 2004 to May 2007**

- Instructor for CSE 2312: Computer Organization and Assembly Language Programming
  - Responsible for course lecture (3 hours/week), designing and grading exams and assignments
  - Students learnt low-level details of x86 platform architecture, devices and assembly language programming in the context of various hands-on programming assignments
- Instructor for CSE 1301: Introduction to C Programming
  - Responsible for course lecture (3 hours/week), designing and grading exams and assignments
  - Students learnt various functional aspects of the C programming language including data types, input and output functions, structures, pointers, arrays, file handling, calling conventions with hands-on programming assignments

Teaching Assistant **May 2006 to August 2006**

- CSE5306: Operating Systems II
  - Tutored students one-to-one and proctored exams
  - Graded assignments and class project deliverables

Teaching Assistant **August 2002 to January 2004**

- CSE2312: Computer Organization and Assembly Language Programming
  - Tutored students one-to-one, proctored and graded exams
  - Prepared and graded assignments and class project deliverables

Hardware and Software Skills

Programming Languages/Tools:

- Assembly (x86 and ARM, 32/64-bit), C, OCaml, Perl, C++, Java, JavaScript, Pascal, UNIX shell scripting, GNU make, and others

Hypervisor Development:

- x86 and ARM hypervisor design and implementation: AMD Secure Virtual Machine (SVM), Intel Virtualization Technology (VT), ARM TrustZone (TZ) and Virtualization Extension Architecture Specficiation (VEAS)
- Dynamic Root-of-Trust/High-Assurance Boot, Nested and Shadow Paging, I/O Virtualization, IOMMU (VT-d,TZPC) and SMM/TZ mode containers
- Principal force behind the design, implementation and verification of the eXtensible and Modular Hypervisor Framework (`http://xmhf.org`). Also explored internals of other open-source hypervisors such as KVM and Xen

System-level Development:

- x86 and embedded ARM architectures: Trusted Platform Module (TPM), custom BIOS development (e.g., coreboot), protected-mode, debugging/SMM/TZ, hardware debug tools, PCI/PCI-E, power management (APM/ACPI), multi-core (SMP), device interrupt interfaces (APIC/IOAPIC/GIC) and others.
- Device drivers: Linux Loadable Kernel Modules (LKM), Windows kernel-mode legacy/WDM drivers, NDIS virtual miniports, and file-system filter drivers
- Linux/Windows kernel development, kernel instrumentation, Windows native applications, disassemblers and emulators.

Software Verification Tools:

- Frama-C, CBMC, SATABS

Version Control and Software Configuration Management:

- DVCS (Mercurial, Git) and VCS (SVN)

Embedded and Real-time Systems:

- Software and hardware development with several MCU and DSP platforms (e.g., Freescale i.MX53, Atmel ATmega MCU's, LPC2148 MCU's, and others)

Operating Systems:

- Microsoft Windows family, Android, Linux

Productivity Applications:

- TEX (LATEX, BIBTEX, PSTricks), Vim, most common productivity packages (for Windows and Linux platforms)

Honors and Awards

- Whos Who Among Students in American Universities and Colleges, University of Texas at Arlington (2005).
- University of Texas at Arlington University Scholar Award, University of Texas at Arlington. (2004 and 2005)
- Cyneta Networks Outstanding Graduate Teaching Assistant Award, Dept. of CSE, University of Texas at Arlington. (2004)
- Graduate Teaching Assistantship, Dept. of CSE, University of Texas at Arlington. (2002 – 2004)
- Masters Dean Fellowship, University of Texas at Arlington. (2002 – 2004)
- National Science Talent Search Examination Prize. India. (1996)
- POWERS, Merit Scholarship, SSLC board, India. (1994)

Talks

- UberSpark: Enforcing Verifiable Object Abstractions for Automated Compositional Security Analysis of a Hypervisor. USENIX Security Symposium, August 2016.
- Design, Implementation and Verification of an eXtensible and Modular Hypervisor Framework. IEEE S&P, May 2013.
- Trustworthy Execution on Mobile Devices: What Security Properties Can My Mobile Platform Give Me?. TRUST, June 2012

- Lockdown: Towards a Safe and Practical Architecture for Security Applications on Commodity Platforms. TRUST, June 2012
- Requirements for an Integrity-Protected Hypervisor on the x86 Hardware Virtualized Architecture. TRUST, June 2010
- Enterprise Security Considerations/ Secure Practices for Distributed Computing and Virtualization. Lockheed Martin Technical Leadership Meet, New Orleans, USA, March 2009. **(Invited)**
- MalTRAK: Tracking and Eliminating Unknown Malware. IEEE ACSAC, December 2008
- WiLDCAT: An Integrated Stealth Environment for Dynamic Malware Analysis. CyLab Seminar Series, CyLab, Carnegie Mellon University, USA, July 2007. **(Invited)**
- Cobra: Fine-grained Malware Analysis using Stealth Localized-executions. IEEE SP, May 2006.
- SPiKE: Engineering Malware Analysis tools using Unobtrusive Binary Instrumentation. ACSC, January 2006
- Stealth Breakpoints. IEEE ACSAC, December 2005.
- SAKTHI: A Retargetable Dynamic Framework for Binary Instrumentation. HICCS, January 2004.

Professional Service

PC/ERC Member: Architectural Support for Programming Languages and Operating Systems (ASPLOS) 2014

PC Member: International Conference on Availability, Reliability and Security (AReS) 2013

PC Member: IEEE International Conference on Risks and Security of Internet and Systems (CRiSIS) 2012

PC Member: IEEE International Conference on Risks and Security of Internet and Systems (CRiSIS) 2011

PC Member: Conference on Decision and Game Theory for Security (GameSec) 2010

PC Member: IEEE International Conference on Risks and Security of Internet and Systems (CRiSIS) 2010

PC Member: Asia-Pacific Signal and Information and Signal Processing Association – Annual Conference 2009

Referee Service

- *IEEE Symposium on Security and Privacy (S&P)*
- *IEEE Transactions on Information Forensics and Security (TIFS)*
- *ACM Transactions on Computer Systems (TOCS)*
- *Journal of Systems and Software (JSS)*
- *ACM Symposium on Operating System Principles (SOSP)*
- *ACM Conference on Computers and Communication Systems (CCS)*
- *European Symposium on Research In Computer Security (ESORICS)*
- *Architectural Support for Programming Languages and Operating Systems (ASPLOS)*
- *Network and Distributed Systems Symposium (NDSS)*
- *Operating System Design and Implementation (OSDI)*

Professional Memberships

Institute for Electrical and Electronics Engineers (IEEE), Member, 2007–present

Assocation of Computing Machinery (ACM), Member, 2007–present