

CONTACT
INFORMATION

4720 Forbes Ave.
2126 CIC
Pittsburgh, PA 15213 USA

Voice: (412) 268-3992
Fax: (412) 268-7828
E-mail: jonmccune@cmu.edu
Web: <http://www.ece.cmu.edu/~jmmccune>

RESEARCH
INTERESTS

Operating system security, virtualization, trustworthy computing (e.g., TCG), security of mobile and wireless devices, including mobile phones, laptops, tablets, and sensor networks.

EDUCATION

Carnegie Mellon University, Pittsburgh, Pennsylvania USA

Ph.D., Electrical and Computer Engineering, January 2009

- Title: “Reducing the Trusted Computing Base for Applications on Commodity Systems”
- Advisors: Adrian Perrig and Michael K. Reiter
- Recipient of the A. G. Jordan Award

M.S., Electrical and Computer Engineering, May 2005

University of Virginia, Charlottesville, Virginia USA

B.S., Computer Engineering, with High Distinction, May 2003

ACADEMIC
EXPERIENCE

Carnegie Mellon University, Pittsburgh, Pennsylvania USA

Research Systems Scientist

February, 2009 – present

Responsibilities include basic research, maintenance and enhancement of research prototypes, and solicitation of research funding. Principal Investigator for research projects including:

- TrustVisor: Efficient TCB Reduction and Attestation
- Isolated Execution on Mobile Devices
- Embedded Processor Root of Trust
- Datacenter Applications of Integrity Measurement Architectures and Trusted Network Connect

Carnegie Mellon University, Pittsburgh, Pennsylvania USA

Graduate Student

September, 2003 – January, 2009

Includes Ph.D. research, graduate level course work and research projects.

Teaching Assistant

2001 – 2008

Duties have included selected lectures, office hours, exam and quiz creation, developing and leading computer lab exercises.

- CMU 18-732 Secure Software Systems, Fall 2008
- CMU 18-730 Introduction to Computer Security, Fall 2005
- CMU 18-731 Network Security, Spring 2005
- UVA CS 216 Program and Data Representation, Fall 2001
- UVA CS 201 Software Development Methods, Spring 2001

PUBLICATIONS

Amit Vasudevan, Emmanuel Owusu, Zongwei Zhou, James Newsome, and Jonathan M. McCune. Trustworthy Execution on Mobile Devices: What security properties can my mobile platform give me? International Conference on Trust and Trustworthy Computing (Trust), June 2012.

Zongwei Zhou, Virgil D. Gligor, James Newsome, and Jonathan M. McCune. Building Verifiable Trusted Path on Commodity x86 Computers. IEEE Symposium on Security and Privacy, May 2012.

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

Jason Franklin, Sagar Chaki, Anupam Datta, Jonathan M. McCune, and Amit Vasudevan. Parametric Verification of Address Space Separation. Conference on Principles of Security and Trust (POST), March 2012.

Yanlin Li, Jonathan M. McCune, and Adrian Perrig. VIPER: Verifying the Integrity of PERipherals' Firmware. ACM Conference on Computer and Communications Security (CCS), October 2011.

Atanas Filyanov, Jonathan M. McCune, Ahmad-Reza Sadeghi, and Marcel Winandy. Uni-directional Trusted Path: Transaction Confirmation on Just One Device. IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), June 2011.

Bryan Parno, Jacob R. Lorch, John R. Douceur, James Mickens, and Jonathan M. McCune. Memoir: Practical State Continuity for Protected Modules. IEEE Symposium on Security and Privacy, May 2011.

Alana Libonati, Jonathan M. McCune, and Michael K. Reiter. Usability Testing a Malware-Resistant Input Mechanism. Network and Distributed System Security Symposium (NDSS), February 2011.

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. International Conference on Trust and Trustworthy Computing (Trust), June 2010.

Yanlin Li, Jonathan M. McCune and Adrian Perrig. SBAP: Software-Based Attestation for Peripherals. International Conference on Trust and Trustworthy Computing (Trust), June 2010.

Jonathan M. McCune, Yanlin Li, Ning Qu, Zongwei Zhou, Anupam Datta, Virgil Gligor, and Adrian Perrig. TrustVisor: Efficient TCB Reduction and Attestation. IEEE Symposium on Security and Privacy, May 2010.

Bryan Parno, Jonathan M. McCune, and Adrian Perrig. Bootstrapping Trust in Commodity Computers. IEEE Symposium on Security and Privacy, May 2010.

Edward J. Schwartz, David Brumley, and Jonathan M. McCune. A Contractual Anonymity System. Network and Distributed System Security Symposium (NDSS), February 2010.

Yue-Hsun Lin, Ahren Studer, Hsu-Chin Hsiao, Jonathan M. McCune, King-Hang Wang, Maxwell Krohn, Phen-Lan Lin, Adrian Perrig, Hung-Min Sun, and Bo-Yin Yang. SPATE: Small-group PKI-less Authenticated Trust Establishment. Conference on Mobile Systems, Applications and Services (MobiSys), June 2009. Best Paper Award.

Bryan Parno, Jonathan M. McCune, Dan Wendlandt, David G. Andersen, and Adrian Perrig. CLAMP: Practical Prevention of Large-Scale Data Leaks. IEEE Symposium on Security and Privacy, May 2009.

Jonathan M. McCune, Adrian Perrig, and Michael K. Reiter. Safe Passage for Passwords and Other Sensitive Data. Network and Distributed System Security Symposium (NDSS), February 2009.

Jonathan M. McCune, Adrian Perrig, and Michael K. Reiter. Seeing is Believing: Using Camera

Phones for Human-Verifiable Authentication. *International Journal of Security and Networks Special Issue on Secure Spontaneous Interaction*. Volume 4, Number 1, 2009.

Chia-Hsin Owen Chen, Chung-Wei Chen, Cynthia Kuo, Yan-Hao Lai, Jonathan M. McCune, Ahren Studer, Adrian Perrig, Bo-Yin Yang, and Tzong-Chen Wu. GAnGS: Gather, Authenticate, and Group Securely. *The International Conference on Mobile Computing and Networking (Mobicom)*, September 2008.

Jason Franklin, Mark Luk, Jonathan M. McCune, Arvind Seshadri, Adrian Perrig, and Leendert Van Doorn. Remote Detection of Virtual Machine Monitors with Fuzzy Benchmarking. In *ACM SIGOPS Operating System Review: Special Edition on Computer Forensics*. Volume 42, Issue 3, April 2008.

Jonathan M. McCune, Bryan Parno, Adrian Perrig, Michael K. Reiter, and Hiroshi Isozaki. Flicker: An Execution Infrastructure for TCB Minimization. *The European Conference on Computer Systems (EuroSys)*, April, 2008.

Jonathan M. McCune, Bryan Parno, Adrian Perrig, Michael K. Reiter, and Arvind Seshadri. How Low Can You Go? Recommendations for Hardware-Supported Minimal TCB Code Execution. *Architectural Support for Programming Languages and Operating Systems (ASPLOS)*, March 2008.

Jonathan M. McCune, Adrian Perrig, Arvind Seshadri, and Leendert van Doorn. Turtles All the Way Down: Research Challenges in User-Based Attestation. *USENIX Workshop on Hot Topics in Security (HotSec '07)*, 2007.

Jonathan M. McCune, Bryan Parno, Adrian Perrig, Michael K. Reiter, and Arvind Seshadri. Minimal TCB Code Execution (Extended Abstract). *IEEE Symposium on Security and Privacy*, May 2007.

Jonathan M. McCune, Stefan Berger, Ramón Cáceres, Trent Jaeger, Reiner Sailer. Shamon: A System for Distributed Mandatory Access Control. *Annual Computer Security Applications Conference (ACSAC)*, December 2006.

Jonathan M. McCune, Adrian Perrig, Michael K. Reiter. Bump in the Ether: A Framework for Securing Sensitive User Input. *USENIX Annual Technical Conference*, May 2006.

Lujo Bauer, Scott Garriss, Jonathan M. McCune, Michael K. Reiter, Jason Rouse, and Peter Rutenbar. Device-Enabled Authorization in the Grey System. *Information Security Conference*, July 2005.

Jonathan M. McCune, Adrian Perrig, and Michael K. Reiter. Seeing is Believing: Using Camera Phones for Human-Verifiable Authentication. *IEEE Symposium on Security and Privacy*, May 2005.

Jonathan M. McCune, Elaine Shi, Adrian Perrig, and Michael K. Reiter. Detection of Denial-of-Message Attacks on Sensor Network Broadcasts. *IEEE Symposium on Security and Privacy*, May 2005.

Cynthia Wong, Stan Bielski, Jonathan M. McCune, and Chenxi Wang. A Study of Mass-mailing Worms. *ACM Workshop on Rapid Malcode (WORM)*, 2004.

John Lach, David Evans, Jon McCune, Jason Brandon. Power-Efficient Adaptable Wireless Sensor Networks. *Military and Aerospace Programmable Logic Devices (MAPLD) International Conference*, September 2003.

Keen Browne, Jon McCune, Adam Trost, et al. Behavior Combination and Swarm Programming.

Springer-Verlag Lecture Notes in Computer Science, 2002.

TECHNICAL
REPORTS

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? Technical Report CMU-CyLab-11-023, Cylab, Carnegie Mellon University, Pittsburgh, PA, November, 2011.

Jonathan M. McCune, Ning Qu, Yanlin Li, Anupam Datta, Virgil D. Gligor, Adrian Perrig. Efficient TCB Reduction and Attestation. Technical Report CMU-CyLab-09-003, Cylab, Carnegie Mellon University, Pittsburgh, PA, March, 2009.

Jonathan M. McCune, Bryan Parno, Adrian Perrig, Michael K. Reiter, and Hiroshi Isozaki. An Execution Infrastructure for TCB Minimization. Technical Report CMU-CyLab-07-018, Cylab, Carnegie Mellon University, Pittsburgh, PA, December 2007.

Jason Franklin, Mark Luk, Jonathan M. McCune, Arvind Seshadri, Adrian Perrig, and Leendert van Doorn. Remote Detection of Virtual Machine Monitors with Fuzzy Benchmarking. Technical Report CMU-CyLab-07-001, Cylab, Carnegie Mellon University, Pittsburgh, PA, January 2007.

Jonathan M. McCune, Adrian Perrig, and Michael K. Reiter. Bump in the Ether: Mobile Phones as Proxies for Sensitive Input. Technical Report CMU-Cylab-05-007, Cylab, Carnegie Mellon University, Pittsburgh, PA, December 2005.

Lujo Bauer, Scott Garriss, Jonathan M. McCune, Michael K. Reiter, Jason Rouse, and Peter Rutenbar. Device-Enabled Authorization in the Grey System. Technical Report CMU-CS-05-111, School of Computer Science, Carnegie Mellon University, February 2005.

Jonathan M. McCune, Adrian Perrig, and Michael K. Reiter. Seeing is Believing: Using Camera Phones for Human-Verifiable Authentication. Technical Report CMU-CS-04-174, Electrical and Computer Engineering Department, Carnegie Mellon University, Pittsburgh, PA, December 2004.

PATENTS

Jonathan M. McCune, Adrian Perrig, Anupam Datta, Virgil D. Gligor, Ning Qu. Methods and Apparatuses for User-Verifiable Trusted Path in the Presence of Malware. International Patent PCT/US2010/040334, WIPO No. WO 2011/037665, pending since June 2010.

Jonathan M. McCune, Virgil D. Gligor, Adrian Perrig, Anupam Datta, Bryan J. Parno, Ning Qu, Amit Vasudevan, Yanlin Li. User-verifiable Execution of Security-Sensitive Code on Untrusted Platforms. Serial No. 12/720,008, pending since June 2010.

PROFESSIONAL
EXPERIENCE

Carnegie Mellon University, Pittsburgh, PA USA

Research Systems Scientist

February, 2009 - present

Research in trusted computing, virtualization, operating systems, systems security, and ad hoc key establishment.

NoFuss Security, Inc, Pittsburgh, PA USA

Co-Founder and President

February, 2010 - present

Service, support, and development for commercialization of trustworthy computing technologies.

VDG, Inc, Pittsburgh, PA USA

Consultant and developer

May, 2010 - April, 2012

Phase II STTR, Army Research Office (ARO) Topic A08-T005, "Trustworthy Execution of Security-Sensitive Code on Un-trusted Systems"

VMware Corporation, Palo Alto, CA USA

Consultant - Trusted Computing

February, 2008 - April, 2008

Studied the applicability of emerging trusted computing technologies to virtualization.

IBM Research, Hawthorne, NY USA

Summer intern - Systems Security

May, 2005 - August, 2005

Designed, implemented, and analyzed an extension to the sHype hypervisor security architecture for the Xen hypervisor. This extension enables *bridging* of mandatory access control (MAC) enforcement between two physically separate systems.

Microsoft Corporation, Redmond, Washington USA

Summer intern - SDET

May, 2002 - August, 2002

Developed two performance benchmarking applications for WinFS based on analysis of customer profiles. Designed, developed, and deployed an application to automate benchmark installation, execution, and result analysis for a cluster of performance-analysis machines. Shared the responsibility of educating several full-time employees who were hired during my time at Microsoft.

UVA Computer Science Department, Charlottesville, Virginia USA

Summer researcher

May, 2001 - September, 2001

Co-founded the UVA RoboCup Soccer Simulator League team. Developed soccer-playing agent using the principles of Swarm programming. Demonstrated the feasibility of achieving desired emergent behavior through combination of many smaller primitives.

PulseNET, Internet Service Provider, Washington, Pennsylvania USA

Assistant technician

May, 2000 - August, 2000

Account maintenance and monitoring on Windows NT and Linux-based web, email, billing, and DNS servers. Technical support to customers employing metropolitan-area wireless connectivity solutions.

SCIENTIFIC TALKS

- TrustVisor: Efficient TCB Reduction and Attestation. (IEEE S&P, Oakland, CA, May, 2010)
- Safe Passage for Passwords and Other Sensitive Data. (NDSS, February 2009)
- How Low Can You Go? Recommendations for Hardware-Supported Minimal TCB Code Execution. (ASPLOS, March 2008)
- Shamon: A System for Distributed Mandatory Access Control (ACSAC, Miami Beach, FL, December, 2006)
- Bump in the Ether: A Framework for Securing Sensitive User Input (Usenix ATC, Boston, MA, June, 2006)
- Seeing is Believing: Using Camera Phones for Human-Verifiable Authentication (IEEE S&P, Oakland, CA, May, 2005)
- Power Efficient Adaptable Sensor Networks (MAPLD, Washington, DC, September, 2003)

PROFESSIONAL SERVICE

- PC Member: 2013 International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS)
- PC Member: 2013 Network and Distributed System Security Symposium (NDSS)
- PC Member: 2012 USENIX Workshop on Hot Topics in Security (HotSec)
- PC Member: 2012 USENIX Security Symposium
- PC Member: TRUST 2012: International Conference on Trust and Trustworthy Computing
- PC Member: 2012 IEEE Symposium on Security and Privacy (Oakland)
- PC Member: 2011 Workshop on Scalable Trusted Computing (STC)
- General Chair: TRUST 2011: International Conference on Trust and Trustworthy Computing
- PC Member: 2011 IEEE Symposium on Security and Privacy (Oakland)
- PC Member: 2011 International Workshop on Security and Privacy in Spontaneous Interaction

and Mobile Phone Use

- PC Member: 2010 Workshop on Scalable Trusted Computing (STC)
- PC Member: 2010 IEEE Symposium on Security and Privacy (Oakland)
- PC Member: 2010 International Workshop on Security and Privacy in Spontaneous Interaction and Mobile Phone Use
- PC Member: TRUST 2010: International Conference on Trust and Trustworthy Computing
- PC Member: 2009 Workshop on Scalable Trusted Computing (STC)

HONORS AND AWARDS

Best paper award for SPATE at MobiSys, 2009

Recipient of the A. G. Jordan Award, for combining outstanding Ph.D. thesis work with exceptional service to the ECE community, 2009

Best paper award for GAnGS at MobiCom, 2008

University of Virginia: graduated with High Distinction in Computer Engineering, 2003

Honorable Mention: Computing Research Association Outstanding Undergraduate Award, 2003

Honorable Mention: ACM Programming Contest World Finals, 2003

UVA CS Department Undergraduate Research Rader Award, 2003

UVA CS Dept. Service Award, 2002

Raven Fellowship Undergraduate Research Grant, 2001

UVA Intermediate Honors for Academic Excellence, 2001

COMPUTER SKILLS

- Languages: C, C++, Java, Perl, Python, Assembly, VHDL
- Operating Systems: Unix/Linux, Windows, Apple OS X, Symbian 6.1/7.0/7.0s/8.0, TinyOS
- Additional Platforms: Nokia Series 60 Phones, Rene Motes, PIC Microcontrollers
- Simulation Packages: GloMoSim
- Applications: L^AT_EX, Unix/Linux shells, common Windows database, spreadsheet, and presentation software