Jonathan M. McCune **Security Researcher, Software Engineer**

CONTACT INFORMATION
(xxx) xxx-xxxx jonmccune@gmail.com
Sunnyvale, CA 94087 USA http://jonmccune.net

SPECIALTIES

Firmware, embedded system, operating system, and virtualization security, trustworthy computing (e.g., TCG), public key infrastructure.

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 for outstanding research and service within CMU ECE

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

University of Virginia, Charlottesville, Virginia USA

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

PROFESSIONAL EXPERIENCE

Google, Inc., Mountain View, California USA

Software Engineer, Security Team **November, 2012 – present**

Design, implementation, deployment, monitoring, and maintenance of systems to enhance production security. Public key infrastructure, trustworthy computing, firmware security.

Carnegie Mellon University, Pittsburgh, Pennsylvania USA

Research Systems Scientist **February, 2009 – October, 2012**

Basic research, software development, and solicitation of research funding. Selected projects:

- eXtensible, Modular Hypervisor Framework (XMHF)
- TrustVisor: Efficient TCB Reduction and Attestation
- Flicker: Minimal TCB Code Execution
- Isolated Execution on Mobile Devices
- Embedded Processor Root of Trust
- Datacenter Applications of Integrity Measurement Architectures and Trusted Network Connect

Open-Source Software

- `xmhf.org`. Hypervisor boot integrity measurement (including dynamic root of trust support on AMD and Intel platforms), cryptographic key management, TrustVisor API and micro-TPM.
- `flickertcb.sf.net`. Isolated execution for security-sensitive code on x86-class systems from AMD and Intel with support for dynamic root of trust, and is compatible with Linux and Windows.
- `github.com/SafeSlingerProject`. Building trusted relationships between people, on the fly, without people having sophisticated knowledge of security protocols.

NoFuss Security, Inc, Pittsburgh, PA USA

Co-Founder and President; Software Engineer **February, 2010 - October, 2012**

Member of three-person engineering team: design, development, and support for commercialization of trustworthy computing technologies. Projects included design and development for the Flicker system (Linux and Windows driver development, AMD CPU microcode loading, Intel VT-d DMA-protection mechanisms, x86 virtual memory), and analysis of COTS hypervisor security.

VDG, Inc, Pittsburgh, PA USA

Software Engineer **May, 2010 - April, 2012**

Phase II STTR, Army Research Office (ARO) Topic A08-T005: Trustworthy Execution of Security-Sensitive Code on Un-trusted Systems. Design and implementation of trustworthy computing functionality for the TrustVisor hypervisor on top of XMHF. Includes boot integrity of XMHF itself via dynamic root of trust and TPM, Micro-TPM API for code running in TrustVisor's protected environment, cryptographic key management, remote attestation protocols, sealed storage APIs, ensuring state continuity for all sensitive state, and regression testing infrastructure.

Wave Systems, Cupertino, CA USA

Consultant and Developer **2010 - 2011**

Boot integrity, support for virtualization.

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.

Selected Publications

Yanlin Li, Jonathan M. McCune, James Newsome, Adrian Perrig, Brandon Baker, and Will Drewry. MiniBox: A Two-Way Sandbox for x86 Native Code. USENIX Annual Technical Conference, June, 2014.

Amit Vasudevan, Sagar Chaki, Limin Jia, Jonathan McCune, James Newsome, and Anupam Datta. Design, Implementation and Verification of an eXtensible and Modular Hypervisor Framework. IEEE Symposium on Security and Privacy, May, 2013.

Emmanuel Owusu, Jorge Guajardo, Jonathan McCune, Jim Newsome, Adrian Perrig, and Amit Vasudevan. OASIS: On Achieving a Sanctuary for Integrity and Secrecy on Untrusted Platforms. ACM Conference on Computer and Communications Security (CCS), November, 2013.

Michael Farb, Yue-Hsun Lin, Tiffany Hyun-Jin Kim, Jonathan M. McCune, and Adrian Perrig. SafeSlinger: Easy-to-Use and Secure Public-Key Exchange. ACM Conference on Mobile Computing and Networking (MobiCom), September 2013.

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.

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.

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.

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.

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.

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.

Selected Technical Reports

Sagar Chaki, Amit Vasudevan, Limin Jia, Jonathan McCune, and Anupam Datta. Design, Development, and Automated Verification of an Integrity-Protected Hypervisor. Technical Report CMU-CyLab-12-017, CyLab, Carnegie Mellon University, Pittsburgh, PA, July, 2012.

Amit Vasudevan, Jonathan M. McCune, and James Newsome. Design and Implementation of an eXtensible and Modular Hypervisor Framework. Technical Report CMU-CyLab-12-014, Cylab, Carnegie Mellon University, Pittsburgh, PA, June, 2012.

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. Issued US Patent 8,832,778 September 2014. International Patent PCT/US2010/040334, WIPO No. WO 2011/037665. Filed June 2010.

Jonathan McCune, Adrian Perrig, Anupam Datta, Virgil Gligor, Yanlin Li, Bryan Parno, Amit Vasudevan, Ning Qu. Methods and apparatuses for user-verifiable execution of security-sensitive code. Issued US Patent 8,627,414 January 2014.

Others pending.

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)

Professional Service

- PC Member: 2015 Usenix Security Symposium
- 2014 National Science Foundation Panelist
- PC Member: 2014 Network and Distributed System Security Symposium (NDSS)
- PC Member: 2014 International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS) External Review Committee

- PC Member: 2014 IEEE Symposium on Security and Privacy (Oakland)
- PC Member: 2014 International Workshop on Trustworthy Embedded Devices (TrustED)
- PC Member: TRUST 2014: International Conference on Trust and Trustworthy Computing
- PC Member: 2013 IEEE Symposium on Security and Privacy (Oakland)
- PC Member: 2013 Usenix Security Symposium
- PC Member: TRUST 2013: International Conference on Trust and Trustworthy Computing
- PC Member: 2013 ACM Conference on Computer and Communications Security (CCS)
- 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: ACM Programming Contest World Finals, 2003

Computer Skills

- Languages: C/C++, x86 Assembly, Python, shell
- Systems software: Linux, Xen, Apple OS X, Windows
- Low-level programming and tools