Joshua Serratelli Schiffman, Ph.D.

1600 Barton Springs Rd. Unit #2103, Austin, TX 78704 USA
+1.609.379.2746 | josh@joshschiffman.org | joshschiffman.org

EDUCATION

Pennsylvania State University, University Park, PA — August 2012
Ph.D., Computer Science and Engineering
Thesis: *Practical System Integrity Verification in Cloud Computing Environments*
Advisor: Trent Jaeger

Pennsylvania State University, University Park, PA — May 2009
M.S., Computer Science and Engineering
Advisor: Trent Jaeger

Pennsylvania State University, University Park, PA — May 2006
B.S., Computer Science and Engineering with Honors and High Distinction
Minors in Mathematics and Japanese Language

EMPLOYMENT

Member of Technical Staff, Security Architect - **Advanced Micro Devices, Inc.**, Austin, TX. — Sept 2012 - Present

- Design and implementation of hardware and software IP to improve the security and capabilities of AMD products.
- Publish research and submit patents on new security architectures, threats, and mitigations, participate in academic and industry committees, and give talks on AMD security architecture.
- Represent AMD in the Trusted Computing Group (Co-Chair of Mobile Platform Working Group, alternate on Technical Committee), Global Platform, and Cyber Security Research Alliance.
- Aided porting TPM 2.0 reference code to AMD's firmware implementation.

Research Intern - **Microsoft Research**, Redmond, WA. — Summer 2011

- Designed and implemented a platform for privacy preserving services. Leveraged Infineon SLE secure hardware, modified Microsoft Hyper-V and designed a Windows Phone 7 application to maintain user privacy in personalized queries. Helped design and evaluate a new multi-client oblivious RAM protocol to protect user privacy in personalized data center services.

Research Intern - **Samsung Electronics R&D**, San Jose, CA. — Summer 2009

- Researched distributed cloud computing application security for mobile devices. Designed and implemented an access control manager for sub-delegation of the OAuth web authorization protocol in consumer electronics.

Research Co-op - **IBM T. J. Watson Research Center**, Hawthorne, NY. — Summer 2008

- Researched access control policies in virtual machine security and stream computing platforms.

Research Assistant to Trent Jaeger - **Pennsylvania State University**, University Park, PA. — 2006 - 2012

- Designed, implemented and evaluated a methods for installing via CD-ROM network-boot to enable simple verification of the installed filesystem's integrity by leveraging the TPM and late-launch (Intel and AMD) CPU features.
- Designed a secure execution monitor for the Linux kernel in Qtopia on OpenMoko (Neo1973 phone and evaluation board) that prevents untrusted binaries from running under critical SELinux labeled processes.
- Built a runtime integrity monitor for both Xen and Linux KVM that verifies remote client specified integrity policies through a service local to the VM's host. Developed a hardware-based VM introspection mechanism to detect integrity violations in hosted VMs. Evaluated architecture on Eucalyptus and OpenStack cloud platforms.
- **Lead Graduate Student** (2010 - 2011) - Primary student organizer of the *Systems and Internet Infrastructure Security* Laboratory. Led weekly meetings of 12+ members, met with PhD and MS candidates individually for mentoring and development of leadership and research skills.

Technical Intern - **Lockheed Martin**, King of Prussia, PA. — Summer 2005, 2006

- Developed web application prototypes for the Coast Guard's Deepwater program. Improved corporate web application for internal requisitions. Automated data entry for the Pennsylvania State Police ArcGIS services.

PUBLICATIONS

JOURNALS

1. T. Moyer, K. Butler, **J. Schiffman**, P. McDaniel, and T. Jaeger. Scalable web content attestation. *IEEE Transactions on Computers*, 17, March 2011.
2. Divya Muthukumaran, **Joshua Schiffman**, Mohamed Hassan, Anuj Sawani, Vikhyath Rao, Trent Jaeger, Protecting the Integrity of Trusted Applications in Mobile Phone Systems, *Security and Communication Networks*, Volume 4, Issue 6, pp 633650, June 2011.
3. **Joshua Schiffman**, Trent Jaeger, and Patrick McDaniel. Network-based Root of Trust for Installation. *IEEE Security & Privacy*, Volume 9, Issue 1, pp 4048, Jan.-Feb. 2011.
4. Trent Jaeger and **Joshua Schiffman**, Outlook: Cloudy with a Chance of Security Challenges and Improvements, *IEEE Security & Privacy*, Volume 8, Issue 1, pp 77-80, Jan.-Feb. 2010
5. Lee, K.C.K., **Schiffman J.**, Zheng, B., Lee, W.C., Leong, H.V. Round-Eye: A system for tracking nearest surrounders in moving object environments, *Journal of Systems and Software*, Volume 80, pp 2063-2076, 2007.

CONFERENCES

6. Yuqiong Sun, Giuseppe Petracca, Trent Jaeger, Hayawardh Vijayakumar and **Joshua Schiffman**. CloudArmor: Protecting Cloud Commands from Compromised Cloud Services. To appear in the *8th IEEE International Conference on Cloud Computing (IEEE CLOUD'15)*, June, 2015.
7. **Joshua Schiffman**, Yuqiong Sun, Hayawardh Vijayakumar, and Trent Jaeger. 2013. Cloud Verifier: Verifiable Auditing Service for IaaS Clouds. In *Proceedings of the 2013 IEEE Ninth World Congress on Services (SERVICES '13)*, Jun. 2013.
8. Hayaward Vijayakumar, **Joshua Schiffman**, and Trent Jaeger. Process Firewalls: Enforcing Safe Resource Access with Attack-Specific Invariants, *Proceedings of the 8th ACM European Conference on Computer Systems*, Apr. 2013.
9. J. Lorch, J. Mickens, B. Parno, M. Raykova, **J. Schiffman**. Toward Practical Private Access to Data Centers via Parallel ORAM, *Proceedings of the 11th USENIX conference on File and Storage Technologies*, Feb. 2013.
10. Hayaward Vijayakumar, **Josh Schiffman**, and Trent Jaeger. STING: Finding Name Resolution Vulnerabilities in Programs, *Proceedings of the 21st USENIX Security Symposium (USENIX Security '12)*, Aug. 2012. *(19% acceptance rate)*
11. **Joshua Schiffman**, Hayaward Vijayakumar, Trent Jaeger. Verifying System Integrity by Proxy, 5th International Conference on Trust and Trustworthy Computing, Jun. 2012.
12. H. Vijayakumar, G. Jakka, S. Rueda, **J. Schiffman**, and T. Jaeger. Integrity Walls: Finding Attack Surfaces from Mandatory Access Control Policies. *In Proceedings of the 7th ACM Symposium on Information, Computer, and Communications Security (AsiaCCS)*, 2012. *To be published. (22% acceptance rate)*
13. Hayawardh Vijayakumar, **Joshua Schiffman**, and Trent Jaeger. A Rose by Any Other Name or an Insane Root? Adventures in Namespace Resolution, *7th European Conference on Computer Network Defense*, September 2010. *(32% acceptance rate)*
14. Patrick Traynor, **Joshua Schiffman**, Thomas La Porta, Patrick McDaniel, Abhrajit Ghosh, and Farooq Anjum, Constructing Secure Localization Systems with Adjustable Granularity, *Proceedings of the IEEE Global Communications Conference (GLOBECOM)*, December, 2010. Miami FL. *(acceptance rate: 35%)*
15. **Joshua Schiffman**, Xinwen Zhang and Simon Gibbs. DAuth: Fine-grained Authorization Delegation for Distributed Web Application Consumers, *POLICY '10: Proceedings of the 2010 IEEE International Symposium on Policies for Distributed Systems and Networks*, July, 2010. Washington, DC. *(acceptance rate 19%)*
16. Sandra Rueda, Boniface Hicks, Dave King, Thomas Moyer, **Joshua Schiffman**, Yogesh Sreenivasan, Trent Jaeger, and Patrick McDaniel. An Architecture for Enforcing End-to-End Access Control Over Web Applications, *SACMAT '10: 15th ACM symposium on Access Control Models and Technologies*, June 2010. Pittsburgh, PA. *(24 % acceptance rate)*
17. **Joshua Schiffman**, Thomas Moyer, Christopher Shal, Trent Jaeger, and Patrick McDaniel. Justifying Integrity Using a Virtual Machine Verifier, *ACSAC '09: Proceedings of the 25th Annual Computer Security Applications Conference*, December 2009. Honolulu, HI. *(19% acceptance rate)*
18. Thomas Moyer, Kevin Butler, **Joshua Schiffman**, Patrick McDaniel, and Trent Jaeger. Scalable Web Content Attestation, *ACSAC '09: Proceedings of the 25th Annual Computer Security Applications Conference*, December 2009. Honolulu, HI. *(19% acceptance rate)*

19. Ken C. K. Lee, **Josh Schiffman**, Baihua Zheng, Wang-chien Lee, Valid Scope Computation for Location-Dependent Spatial Query in Mobile Broadcast Environments, *17th ACM Conference on Information and Knowledge Management*, October 2008. (17% acceptance rate)
20. Divya Muthukumaran, Anuj Sawani, **Joshua Schiffman**, Brian M. Jung, Trent Jaeger, Measuring Integrity on Mobile Phone Systems, *SACMAT '08: 13th ACM symposium on Access Control Models and Technologies*, June 2008. *(25 % acceptance rate)*
21. Luke St.Clair, **Joshua Schiffman**, Trent Jaeger, and Patrick McDaniel, Establishing and Sustaining System Integrity via Root of Trust Installation, *ACSAC '07: 23rd Annual Computer Security Applications Conference*, December 2007. *(22 % acceptance rate)*
22. Ken C. K. Lee, **Josh Schiffman**, Baihua Zheng, Wang-Chien Lee and Hong Va Leong. Tracking Nearest Surrounders in Moving Object Environments. In *IEEE International Conference on Pervasive Services*, 2006.

WORKSHOPS

23. **Joshua Schiffman** and David Kaplan, The SMM Rootkit Revisited: Fun with USB, *2nd International Workshop on Emerging Cyberthreats and Countermeasures (ECTCM '14)*, Sept. 2014.
24. **Joshua Schiffman**, Thomas Moyer, Hayawardh Vijayakumar, Trent Jaeger, and Patrick McDaniel, Seeding Clouds with Trust Anchors. *2nd ACM Cloud Computing Security Workshop*, October 2010. Chicago, IL
25. Xinwen Zhang, **Joshua Schiffman**, Simon Gibbs, Anugeetha Kunjithapatham, and Sangoh Jeong. Securing Elastic Applications on Mobile Devices for Cloud Computing, *1st ACM Cloud Computing Security Workshop*, November 2009. Chicago, IL.
26. William Enck, Sandra Rueda, Yogesh Srdeenivasan, **Joshua Schiffman**, Luke St. Clair, Trent Jaeger, and Patrick McDaniel. Protecting Users from 'Themselves', *Proceedings of the 1st ACM Computer Security Architectures Workshop*, November 2007. Alexandria, VA.

TECHNICAL REPORTS

27. J. R. Lorch, J. Mickens, B. Parno, M. Raykova, and **J. Schiffman**. Toward practical private access to data centers via parallel oram. Cryptology ePrint Archive, Report 2012/133. `http://eprint.iacr.org/2012/133`.
28. Kevin Butler, Stephen McLaughlin, Thomas Moyer, **Joshua Schiffman**, Patrick McDaniel, and Trent Jaeger. Firma: Disk-Based Foundations for Trusted Operating Systems. Technical Report NAS-TR-0114-2009, Networking and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, May 2009.
29. **Joshua Schiffman**, H. Vijayakumar, and T. Jaeger. Eliminating remote attestation via integrity verification proxies. Technical Report NAS-TR-0152-2011, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, Sept. 2011.

PATENTS

1. Samsung Electronics Co., Ltd.: **Joshua Schiffman** et al, "Securely Using Service Providers in Elastic Computing Systems and Environments," U.S. Patent Application Number: 20110004916 *(April 22, 2010)*

INVITED TALKS

1. Verifying System Integrity by Proxy, *Imperial College London*, September 15, 2014. London, UK.
2. Practical Verification of System Integrity In Cloud Computing Environments, *Trusted Infrastructure Workshop (TIW '13*, June 5, 2013.
3. Towards Practical Attestation: Challenges and Opportunities, *Trusted Infrastructure Workshop (TIW '12)*, June 10, 2010. Pittsburgh, PA.

HONORS

- ACM CCS Conference Student Travel Grant Award 2009
- ACM CCS Workshop Student Travel Grant Awards 2009, 2010
- University Graduate Fellowship Award 2008-2009
- USENIX Association Student Travel Stipend 2007-2011
- IEEE Security and Privacy Travel Grant 2009
- Penn State College of Engineering Fellowship 2006-2007

- ACM SIGMOD Undergraduate Scholarship 2006
- Admitted to the Phi Kappa Phi Honors Society 2006
- Lockheed Martin Engineering Scholars Award 2003

SERVICE

PROGRAM COMMITTEES

- ACM Symposium on Information, Computer and Communications Security (ASIACCS) 2014, 2015
- ACSA Annual Computer Security Applications Conference (ACSAC) 2013, 2014
- International Workshop on Emerging Cyberthreats and Countermeasures (ECTCM) 2015
- ACM Workshop on Scalable Trusted Computing (STC) 2012
- International Workshop on Security (IWSEC) 2012

STANDARDS BODIES

- Co-Chair - TCG Mobile Platform Working Group 2015 - Present
- Alternate - TCG Technical Committee 2014 - Present
- Member - Global Platform (GP) 2014 - Present

REVIEWER

- IEEE Transactions on Computers
- IEEE Transactions on Dependable and Secure Computing
- ACM SIGCOMM's Computer Communication Review
- Computer Networks Journal

EXTERNAL REVIEWER

- USENIX Security Symposium
- ACM Computer and Communications Security Conference (CCS)
- IEEE Symposium on Security and Privacy
- ISOC Network and Distributed System Security Symposium (NDSS)
- ACM Annual Computer Security Applications Conference (ACSAC)
- European Conference on Computer Systems (Eurosys)
- ACM Symposium on Access Control Models and Technologies (SACMAT)
- ICST SecureComm
- Information Security Conference
- ACM Workshops: Scalable Trusted Computing (STC), Virtual Machine Security (VMSec), Cloud Computing Security Workshop (CCSW), SafeConfig
- USENIX Workshops: HotSec, HotCloud, WOOT
- International Workshop on Security in Systems and Networks
- IEEE International Workshop on Security in Software Engineering

PROFESSIONAL AFFILIATIONS

- The Association for Computing Machinery (ACM)
- The Institute of Electrical and Electronics Engineers (IEEE)
- USENIX Advanced Computing Systems Association (USENIX)