
Joshua Serratelli Schiffman

Ph.D. Candidate

Department of Computer Science and Engineering ◊ Pennsylvania State University

Office : 344 IST Building ◊ University Park, PA 16802 ◊ (717) 645-5731

Email : jschiffm@cse.psu.edu ◊ **Homepage**: www.joshschiffman.org

EDUCATION

- Pennsylvania State University**, University Park, PA *Expected: May 2012*
Ph.D., Computer Science and Engineering
Advisor: Trent Jaeger
- Pennsylvania State University**, University Park, PA 2009
M.S., Computer Science and Engineering
Thesis: Efficient and Scalable Verification of Distributed System Integrity Using SHIMA
Advisor: Trent Jaeger
- Pennsylvania State University**, University Park, PA 2006
B.S., Computer Science and Engineering with Honors and High Distinction
Minors in Mathematics and Japanese Language

RESEARCH EXPERIENCE

- Research Assistant** to Trent Jaeger, *Pennsylvania State University*, University Park, PA. 2006 - Present
- Designed, implemented and evaluated a method for installing systems both via CD-ROM and over network-boot that enables simple verification of the installed filesystem's integrity. Leveraged the Trusted Platform Module and late-launch features of recent CPUs to provide a measured installation environment.
 - Designed a secure execution monitor for the Linux kernel that prevents untrusted binaries from running under critical SELinux labeled processes. Implemented monitor for Qtopia on OpenMoko Neo1973 phone and an evaluation board.
 - Built a runtime integrity monitor for both Xen and Linux KVM virtual machine hosts that enables remote clients and administrators to specify an integrity policy that is monitored on their behalf by 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**, *Systems and Internet Infrastructure Security (SIIS) Laboratory* Aug. 2010 - Dec. 2011
Pennsylvania State University, University Park, PA.
- Performed daily administrative and logistical duties for the SIIS lab. Ran weekly meetings of 12+ members, met with students individually for mentoring and development of leadership and research skills.

INDUSTRIAL EXPERIENCE

- Research Intern** *Microsoft Research*, Redmond, WA. Summer 2011
- Designed and implemented 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.
- 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. Thomas Moyer, Kevin Butler, **Joshua Schiffman**, Patrick McDaniel, and Trent Jaeger. Scalable Web Content Attestation. *IEEE Transactions on Computers*. 2011. *To appear*.
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*, 9(1):4048, Jan.-Feb. 2011.
4. Trent Jaeger and **Joshua Schiffman**, Outlook: Cloudy with a Chance of Security Challenges and Improvements, *IEEE Security & Privacy Magazine*, 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 surroundings in moving object environments, *Journal of Systems and Software*, 80:2063-2076, 2007.

CONFERENCES

6. 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)
7. 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%)
8. **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%)
9. 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)
10. **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)
11. 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)
12. 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)
13. 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)
14. 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)
15. 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

16. **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
17. 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.

-
18. 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

19. 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.
20. Patrick Traynor, **Joshua Schiffman**, Thomas La Porta, Patrick McDaniel, Abhrajit Ghosh, and Farooq Anjum, Constructing Secure Localization Systems with Adjustable Granularity, Technical Report NAS-TR-0084-2007, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, December 2007. (Superseded by Constructing Secure Localization Systems with Adjustable Granularity)
21. **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.

MISCELLANEOUS

22. **Joshua Schiffman**, USENIX Security Symposium Conference Summaries. *USENIX ;login Magazine*, Dec. 2010.
23. **Joshua Schiffman**, USENIX Security Symposium Conference Summaries. *USENIX ;login Magazine*, Dec. 2008.

PATENTS FILED

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. Towards Practical Attestation: Challenges and Opportunities, *Trusted Infrastructure Workshop*, June 10, 2010. Pittsburgh, PA.

AWARDS AND 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

EXTERNAL SERVICE

Years omitted for brevity.

Reviewer:

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

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