Joel H. W. Weinberger

Contact Information

723 Soda Hall
Computer Science
UC Berkeley
Berkeley, CA 94720 USA

Mobile: (415) 309-0684
E-mail: jww@cs.berkeley.edu
Website: `http://www.cs.berkeley.edu/~jww`

Research Interests

Web security, systems security, privacy, programming languages, software engineering

Education

University of California, Berkeley, Berkeley, California USA

Ph.D. Graduate Student, Computer Science, 2008-2012
Advised by Dawn Song

Brown University, Providence, Rhode Island USA

M.S., Computer Science, May, 2007
B.S., Computer Science & History, May 2007

Honors and Awards

Brown University: graduated Magna Cum Laude, Phi Beta Kappa, 2007

Academic Experience

University of California, Berkeley

Graduate Student Researcher **September, 2008 - present**
Includes current Ph.D. research and coursework with a focus on security.

Graduate Student Instructor **January, 2010 - May, 2010, January 2012 - present**
Graduate student instructor for advance undergraduate computer security course. Shared responsibility for leading sections, developing coursework including homeworks and projects, and grading.

Course Work
Security, Program Analysis, Programming Languages, Network Security, Systems, Cryptography, Intellectual Property Law, Surveillance and Society

Brown University

Teaching Assistant **September, 2005 - present**
Held office hours, created and graded assignments, and led lab sections for Computer Systems, Computer Security, and Operating Systems courses.

Selected Course Work
Operating Systems, Programming Languages, Dynamic Access Control and Verification, Combinatorial Optimization, Computer Networks

Refereed Publications

Weinberger, J., Saxena, P., Akhawe, D., Finifter, M., Shin, R., Song, D. *A Systematic Analysis of XSS Sanitization in Web Application Frameworks.* European Symposium on Research in Computer Security (ESORICS), 2011.

Weinberger, J., Barth, A., Song, D. *Towards Client-side HTML Security Policies.* Workshop on Hot Topics in Computer Security (HotSec), 2011.

Felt, A., Finifter, M., Weinberger, J., Wagner, D. *Diesel: Applying Privilege Separation to Database Access.* ACM Symposium on Information, Computer and Communications Security (ASIACCS), 2011.

Finifter, M., Weinberger, J., and Barth, A. *Preventing Capability Leaks in Secure JavaScript Subsets.* Network and Distributed System Security Symposium (NDSS), 2010.

Barth, A., Weinberger, J., and Song, D. *Cross-Origin JavaScript Capability Leaks: Detection, Exploitation, and Defense.* USENIX Security Symposium, 2009.

Gordon, C., Meyerovich, L., Weinberger, J., and Krishnamurthi, S. *Composition with Consistent Updates for Abstract State Machines.* International ASM Workshop, 2007.

Technical Reports

Swamy, N., Weinberger, J., Chen, J., Livshits, B., Schlesinger, C. *Monadic Refinement Types for Verifying JavaScript Programs.* Microsoft Research Technical Report, 2012.

Meyerovich, L., Weinberger, J., Gordon, C., and Krishnamurthi, S. *ASM Relational Transducer Security Policies.* Brown University Technical Report CS-05-12, 2006.

Research

Web Application Script Type-checking for Security
Using dependent typing and refinement typing to statically enforce security properties of JavaScript. Evaluating the power of these techniques on real web scripts, focusing on web browser extensions.

Web Application Sanitization
Examining how web applications perform sanitization, both on the server and on the client. Looking at ways of identifying sanitization checks on the server and client. Building tools to create and enforce sanitization policies in web applications.

JavaScript Heap Analysis
Instrumenting a JavaScript engine to map JavaScript objects and their relationships to one another. Using this tool to verify the security of web browsers and web applications, as well as finding vulnerabilities in them.

Database Privilege Separation
Creating a system for applying the principle of least privilege to software database access. Allows for a single database connection to be securely shared among program modules while guaranteeing minimum access rights to the database for each module.

Verification of Web Programs
Modeled an access control system for a web application and developed an atomic update module operator for Abstract State Machines (ASMs).

Professional Experience

Coverity, San Francisco, California, USA

Researcher **June 2012 - present**
Office of the CTO working on security technology research. Focusing on next-generation analysis of web applications. Looking at ways to connect server static analysis with client analysis.

Microsoft Research, Redmond, Washington USA

Research Intern **June 2011 - August 2011**
Intern in the Research in Software Engineering (RiSE) group, working with Juan Chen, Ben Livshits, and Nikhil Swamy. Focused on type checking of JavaScript using F*, an F♯-like language with dependent and refinement typing. Worked on statically enforcing complex security policies on web applications through the type system, focusing on browser extensions. Built a compiler from JavaScript to F* and worked on type checking on resulting code for correctness and security properties.

Sun Microsystems, San Francisco, California USA

Software Engineer **July 2007 - July 2008**
Full-time software engineer in the Fishworks advanced development team on Sun Storage 7000 NAS

products. Worked on iSCSI and FTP integration, clustering interface support, and appliance stack management. Worked on operating system, application, and AJAX web development.

VMware, Palo Alto, California USA

Intern Software Engineer **June 2006 - August 2006**

Intern in the VMware ESX Core Kernel group. Developed shared memory infrastructure and signal handling capabilities.

Technical Skills

Programming Languages: C/C++, Java, JavaScript, F#, OCaml, Python, BASH, Scheme, HTML

Computer Systems: Linux, Solaris, MacOS X, Windows

Interests

Rock climbing, tap dance, skiing (alpine and water), coffee, running, road biking, history