Benjamin Livshits

Gates Building, Room 406, Stanford, CA 94305
livshits@cs.stanford.edu • http://www.stanford.edu/~livshits/

Research Interests

Programming languages and tools for program analysis • Static and dynamic analysis techniques for bug detection • Static and dynamic analysis techniques for finding security vulnerabilities in programs • Pointer analysis and its precision • Role of soundness and precision in static analysis tools • Failure and vulnerability recovery in complex systems, especially Web services • Using alternative sources such as revision histories for program understanding • Applying AI, data mining, and statistical learning techniques to the discovery of correct and erroneous program behavior

Education

Stanford University.
Pursuing a Ph.D. in Computer Science. *2002 — present*
Thesis: *Improving Software Security with Precise Static and Dynamic Analysis.*
Expected graduation date: Spring 2006.

Stanford University.
M.S. in Computer Science. *1999 — 2001*
Degree specialization: *Software theory.*
Research topic: *Program Representation for Bug Detection.*

Cornell University.
B.A. in Computer Science and Mathematics,
Summa Cum Laude with Distinction in Computer Science. *1999*
Undergraduate research project: *A Mostly-copying Garbage Collector for Java.*
GPA in major subjects: 4.09, overall GPA: 4.03.

Publications

Representative Recent Publications:

- **Finding Security Vulnerabilities in Java Applications with Static Analysis**, Benjamin Livshits and Monica S. Lam, In Proceedings of the Usenix Security Symposium, Baltimore, Maryland, *August 2005*
- **Finding Application Errors and Security Flaws Using PQL: a Program Query Language**, Michael Martin, Benjamin Livshits, and Monica S. Lam, In Proceedings of the 20th Annual ACM Conference on Object-Oriented Programming, Systems, Languages, and Applications (OOPSLA 2005), San Diego, California, *October 2005*
- **DynaMine: Finding Common Error Patterns by Mining Software Revision Histories**, Benjamin Livshits and Thomas Zimmermann, In Proceedings of the ACM SIGSOFT Symposium on the Foundations of Software Engineering (FSE 2005), Lisbon, Portugal, *September 2005* (an extended version is currently under preparation for TOSEM)
- **Reflection Analysis for Java**, Benjamin Livshits, John Whaley and Monica S. Lam, In Proceedings of the Third Asian Symposium on Programming Languages and Systems, (APLAS 2005), Tsukuba, Japan, *November 2005*

Other Peer-reviewed Publications:

- **Mining Additions of Method Calls in ArgoUML**, Thomas Zimmerman, Silvia Breu, Christian Lindig, and Benjamin Livshits, International Workshop on Mining Software Repositories Challenge, Shanghai, China, *May, 2006*
- **Defining a Set of Common Benchmarks for Web Application Security**, Benjamin Livshits, Position paper on Stanford SecuriBench for the Workshop on Defining the State of the Art in Software Security Tools, Baltimore, *August 2005*
- **Locating Matching Method Calls by Mining Revision History Data**, Benjamin Livshits and Thomas Zimmermann, In Proceedings of the Workshop on the Evaluation of Software Defect Detection Tools, Chicago, Illinois, *June 2005*
- **Context-Sensitive Program Analysis as Database Queries**, Monica S. Lam, John Whaley, Benjamin Livshits, Michael Martin, Dzintars Avots, Michael Carbin, Christopher Unkel, In Proceedings of Principles of Database Systems (PODS 2005), Baltimore, Maryland, *June 2005*
- **Improving Software Security with a C Pointer Analysis**, Dzintars Avots, Michael Dalton, Benjamin Livshits, Monica S. Lam, In Proceedings of the 27th International Conference on Software Engineering (ICSE 2005), *May 2005*
- **Turning Eclipse Against Itself: Finding Bugs in Eclipse Code Using Lightweight Static Analysis**, Benjamin Livshits, In Eclipsecon '05 Research Exchange, *March 2005*
- **Finding Security Errors in Java Applications Using Lightweight Static Analysis**, Benjamin Livshits, In Annual Computer Security Applications Conference (ACSAC 2005), Work-in-Progress Report, *November 2004*
- **Tracking Pointers with Path and Context Sensitivity for Bug Detection in C Programs**, Benjamin Livshits and Monica S. Lam, In Proceedings of the 11th ACM SIGSOFT International Symposium on the Foundations of Software Engineering (FSE 2003), Helsinki, Finland, *September 2003*

Technical Reports:

- **Turning Eclipse Against Itself: Improving the Quality of Eclipse Plugins**, Benjamin Livshits, Stanford University Technical Report, *September 2005*
- **Reflection Analysis for Java**, Benjamin Livshits, John Whaley, and Monica S. Lam, Stanford University Technical Report, *October 2005*
- **Finding Security Vulnerabilities in Java Applications with Static Analysis**, Benjamin Livshits and Monica S. Lam, Stanford University Technical Report, *August 2005*

Other Articles*:

- **Looking for Memory Leaks**, An article on detecting memory leaks in Java for Oracle Developer Network as part of the Mastering J2EE Application Development Series, *January 2005*

Unpublished Research Manuscripts:

- **Unsupervised Web Page Clustering**, A graduate research project in natural language processing at Stanford (CS 224N), *Spring 2000*
- **Applications of Cache-conscious Data Layout to Copying Garbage Collection**, A graduate research project in compilers (CS 612) at Cornell University, *May 1999*

*Links to PDF versions of these papers are available from my home page mentioned above.

- **MCC for Java**, An undergraduate research project at Cornell on a mostly-copying garbage collector for Java, *May 1999*

Research Activities

- **Participant of Dugstuhl Seminar**, Dugstuhl, Germany. *June 2005.*
  Participated in a week-long "Multi-version program analysis" seminar (seminar № 05261). Gave an overview of work we did on applying data mining techniques for revision history repositories to the task of finding good error patterns to check.

- **Visiting Researcher**, Tel Aviv University, Israel. *Spring 2004.*

  Worked with Prof. Mooly Sagiv on a project to statically verify conformance to interface requirements for common interfaces. For example, there are often dozens of classes implementing the `java.util.Collection` interface in large Java systems. However, not all of them satisfy the requirements imposed by the interface contract.

  Preliminary results were presented at Berkeley in talk entitled "A Case Study in Automatic Assume-Guarantee Reasoning Proving Conformance to Collection Interface Requirement"

- **Conference reviewer.** Was invited as an informal reviewer for the OOPSLA 2006 conference and the TOPLAS journal.

Teaching Activities

I was a teaching assistant for the following courses:

- **CS 243**: Advanced Compiling Techniques *Winter 2006*
  Taught at Stanford under the supervision of Prof. Jeff Ullman & Wei Li

- **CS 242**: Programming Languages *Fall 2005*
  Taught at Stanford under the supervision of Prof. John Mitchell

- **CS 343**: Advanced Topics in Compilers *Spring 2002*
  Taught at Stanford under the supervision of Prof. Monica Lam

- **CS 280**: Discrete Structures *Spring 1999*
  Taught at Cornell under the supervision of Prof. David Gries

Students Supervised

In the course of my Ph.D. research I supervised several advanced undergraduate, master's, and junior graduate students. These typically were fruitful collaborations, resulting in interesting research results and publications.

- **Chang-Seo Park.** *Spring 2006 — present*
  Topic: Finding Memory Leaks in C and C++ Using Static Analysis (Take 2).

  Our research group at Stanford has had an ongoing interest in static analysis for finding memory leaks. This work has resulted in two publications to date, including "A Practical Flow-Sensitive and Context-Sensitive C and C++ Memory Leak Detector" published in PLDI 2003. As a widely-used long-running application, Mozilla Firefox represents an attractive target for memory leak analysis. The size of the applications will also allow us to study the sources of false positives in more detail. In particular, is is widely believed that the right amount of predicate sensitivity will eliminate a great number of false positives.

- **Naeim Semsarilar.** *Winter 2006 — present*
  Topic: Using Machine Learning to Improve Specification for Bug Finding Tools.

  Coming up with a proper specification of what represents a bug in a program is a surprisingly difficult task. Even if the analysis approach is sound, more often than not the bug specification remains incomplete. The goal of this project is to explore the use of machine learning techniques to learn patterns from object run-time traces. In particular, our focus is on automatically obtaining complete specifications for security bugs in Java such as SQL injections, cross-site scripting and other similar sorts of attacks.

- **Jean-Gabriel Morard.** *Fall 2005 — present*
  Topic: Using POBDDs to Improve the Scalability of Program Analysis.

  The goal of this research is to use partitioned ordered BDD data structures to improve the scalability of `bddbddb`, a program analysis tool used within the SUIF group. POBDDs were previously successfully applied to the task of hardware verification and resulted in significant scalability improvements compared to regular BDDs. This research is sponsored by Fujitsu Labs.

- **Will Robinson and Ben De'Angelo.** *Summer 2003*
  Topic: Integrating Program Analysis Results with Eclipse.

  The goal of this project was to explore the use of Eclipse as a front end for a variety of program analysis and bug finding tools being developed in the SUIF group at Stanford. This research culminated in a paper presented at OOPSLA: "Integrating software productivity tools into Eclipse," by Will Robinson, Ben D'Angelo, OOPSLA Workshop on Eclipse Technology eXchange, 2003.

Industry Experience

- **Yahoo! Inc.**, Yahoo! Research in collaboration with the Data Mining Group.
  Software Design Engineer. *Summer 2002*

  - Created a data mining system for modeling usage data that Yahoo! collects for their advertising campaigns in order to estimate the relative effectiveness of different means of advertising and to improve the performance of individual ad campaigns.
  - This work included initial research, algorithm development, system implementation, and evaluation of the system with multiple large data sets.
  - Resulting algorithm and experimental results were presented to a large technical staff group at Yahoo! and met with a positive response.

- **Netscape Corporation**, JavaScript Language & Compiler Group.
  Software Design Engineer. *Summer, Winter 1998*

  - Designed and implemented PerlConnect, a package that provides means for interaction between JavaScript and Perl. PerlConnect is similar to LiveConnect, a Netscape product that allows JavaScript and Java talk to one another. It is part of Mozilla open source initiative. PerlConnect is now used as part of Ginger Alliance (`http://www.gingerall.cz`).
  - Wrote a JavaScript shell similar to `tcsh` and other UNIX shells. Implemented compiler optimization for the JavaScript engine written in Java.
  - Wrote a testing framework for JavaScript embedders API written in C.

- **Intel Corporation**, Networked Systems Management Group.
  Software Engineer. *Summer 1997*

– Designed and implemented a wide range of advanced CGI applications for the Web in Perl. Applications were designed to monitor various network management tasks. Developed full-featured Web-based database applications with MS Access as a back end.

References

Prof. Monica Lam
Stanford University
Gates Building, Room 307
353 Serra Mall
Stanford CA 94305
(650) 725-3714
lam@cs.stanford.edu

Prof. Alex Aiken
Stanford University
Gates Building, Room 411
353 Serra Mall
Stanford University
(650) 725-3359
aiken@cs.stanford.edu

Prof. Andreas Zeller
Saarland University
Dept. of Informatics
Postfach 15 11 50
66041 Saarbrcken, Germany
+49 (0)681 302-64011
zeller@cs.uni-sb.de

Prof. Shmuel (Mooly) Sagiv
Tel-Aviv University
School of Computer Science
Schreiber 317
Tel-Aviv 69978, Israel
+972-3-6407606
msagiv@post.tau.ac.il

Honors & Awards

- Winner of an NSF Graduate Fellowship
- National Deans List, Cornell University, all semesters
- Golden Key National Honor Society

Outside Interests

- Classical guitar
- Hiking and camping, a member of the Stanford Redwood Club
- Badminton (competitive level)
- Table tennis (semi-competitive level)
- Photography (semi-professional, worked as a a part-time newspaper photojournalist), some of my work is available from http://www.oberon-imaging.com.
- Tutoring high school students