William G.J. Halfond

Georgia Institute of Technology
266 Ferst Drive, Room 2405
Atlanta, GA 30332-0765

Phone: (404) 788-5653
whalfond@cc.gatech.edu
http://www.cc.gatech.edu/~whalfond

Education

2002-2009 **Georgia Institute of Technology** ..... Atlanta, GA

8/2009 Ph.D. in Computer Science
Thesis: Web Application Modeling for Testing and Analysis.
Advisor: Alessandro Orso.

5/2004 M.S. in Computer Science, GPA: 3.91

1998-2002 **University of Virginia** ..... Charlottesville, VA
B.S. in Computer Science with High Distinction
Senior Thesis: Simulation of the Joint Battlespace Infosphere.
Advisor: John Knight.

Research Interests

Web applications, testing, program analysis, and security.

Refereed Journal Publications

[1] William G.J. Halfond, Alessandro Orso, and Panagiotis Manolios. WASP: Protecting Web Applications Using Positive Tainting and Syntax-Aware Evaluation. *IEEE Transactions on Software Engineering (TSE)*, 2008, Vol 34:1, pages 65–81.

Refereed Conference Publications

[2] William G.J. Halfond, Saswat Anand, and Alessandro Orso. Precise Interface Identification to Improve Testing and Analysis of Web Applications. In *Proceedings of the International Symposium on Testing and Analysis (ISSTA)*. Chicago, Illinois, July 2009. To Appear. **ACM Distinguished Paper Award**

[3] William G.J. Halfond, Shauvik Roy Choudhary, and Alessandro Orso. Penetration Testing with Improved Input Vector Identification. In *Proceedings of the IEEE International Conference on Software Testing (ICST)*. Denver, Colorado, April 2009. Acceptance rate: 33%.

[4] William G.J. Halfond and Alessandro Orso. Automated Identification of Parameter Mismatches in Web Applications. In *Proceedings of the ACM SIGSOFT Symposium on the Foundations of Software Engineering (FSE)*, pages 181–191, Atlanta, Georgia, November 2008. Acceptance rate: 20%.

[5] William G.J. Halfond and Alessandro Orso. Improving Test Case Generation for Web Applications Using Automated Interface Discovery. In *Proceedings of the European Software Engineering Conference and ACM SIGSOFT Symposium on the Foundations of Software Engineering (ESEC/FSE)*, pages 145–154, Dubrovnik, Croatia, September 2007. Acceptance rate: 17%.

[6] William G.J. Halfond, Alessandro Orso, and Panagiotis Manolios. Using Positive Tainting and Syntax-Aware Evaluation to Counter SQL Injection Attacks. In *Proceedings of the ACM SIGSOFT Symposium on the Foundations of Software Engineering (FSE)*, pages 175–185, Portland, Oregon, November 2006. Acceptance rate: 20%.

[7] William G.J. Halfond and Alessandro Orso. Command-Form Coverage for Testing Database Applications. In *Proceedings of the 21st IEEE and ACM International Conference on Automated Software Engineering (ASE)*, pages 69–78, Tokyo, Japan, September 2006. Acceptance rate: 18%.

[8] William G.J. Halfond and Alessandro Orso. Preventing SQL Injection Attacks Using AMNESIA. In *Proceedings of the 28th IEEE and ACM SIGSOFT International Conference on Software Engineering (ICSE)*, Formal Demo, pages 795-798, Shanghai, China, May 2006. Acceptance rate: 22%.

[9] William G.J. Halfond, Jeremy Viegas, and Alessandro Orso. A Classification of SQL-Injection Attacks and Countermeasures. In *Proceedings of the International Symposium on Secure Software Engineering (ISSSE)*, pages 12–23, McLean, VA, March 2006. Acceptance rate: 40%.

[10] William G.J. Halfond and Alessandro Orso. AMNESIA: Analysis and Monitoring for NEutralizing SQL-Injection Attacks. In *Proceedings of the 20th IEEE and ACM International Conference on Automated Software Engineering (ASE)*, pages 174–183, Long Beach, CA, November 2005. Acceptance rate: 10%.

Refereed Workshop Publications

[11] William G.J. Halfond and Alessandro Orso. Combining Static Analysis and Runtime Monitoring to Counter SQL-Injection Attacks. In *Proceedings of the Third International Workshop on Dynamic Analysis (WODA)*, pages 22–28, St. Louis, MO, May 2005. Acceptance rate: 52%.

Other Publications

[12] William G.J. Halfond. Web Application Modeling for Testing and Analysis. In *Proceedings of the ACM SIGSOFT Symposium on the Foundations of Software Engineering (FSE)*, Doctoral Symposium, Atlanta, Georgia, November 2008.

[13] William G.J. Halfond and Alessandro Orso. Detection and Prevention of SQL Injection Attacks. *Malware Detection*, Series: Advances in Information Security, Springer, Vol. 27, M. Christodorescu, S. Jha, D. Maughan, D. Song, C. Wang (Eds.), 2007, XII. Invited.

Presentations

7/2009 **International Symposium on Software Testing and Analysis** ..... Chicago, IL
Precise Interface Identification to Improve Testing and Analysis of Web Applications

4/2009 **International Conference on Software Testing** ..... Denver, CO
Penetration Testing with Improved Input Vector Identification
Best Presentation Award

4/2009 **Dagstuhl Seminars - Web Application Security** ..... Dagstuhl, Germany
Improving Web Application Security with Program Analysis

11/2008 **Foundations of Software Engineering** ..... Atlanta, GA

Automated Identification of Parameter Mismatches in Web Applications
Best Student Presentation Award

11/2008 **Foundations of Software Engineering, Doctoral Symposium** .... Atlanta, GA
Web Application Modeling for Testing and Analysis

9/2007 **Foundations of Software Engineering** ..... Dubrovnik, Croatia
Improving Test Case Generation for Web Applications Using Automated Interface Discovery

11/2006 **Foundations of Software Engineering** ..... Portland, OR
Using Positive Tainting and Syntax-Aware Evaluation to Counter SQL Injection Attacks

5/2006 **International Conference on Software Engineering** ..... Shanghai, China
Preventing SQL Injection Attacks Using AMNESIA

3/2006 **International Symposium on Secure Software Engineering** ..... McLean, VA
A Classification of SQL-Injection Attacks and Countermeasures

11/2005 **Automated Software Engineering** ..... Long Beach, CA
AMNESIA: Analysis and Monitoring for NEutralizing SQL-Injection Attacks

5/2005 **Workshop on Dynamic Analysis** ..... St. Louis, MO
Combining Static Analysis and Runtime Monitoring to Counter SQL-Injection Attacks

Work Experience

Summer 2007 **Research Intern**, Microsoft ..... Seattle, WA
Developed technique for automatic instrumentation of AJAX-based web applications.

2005-present **Research Assistant**, College of Computing, Georgia Tech ..... Atlanta, GA

2004-2005 **Research Assistant**, Georgia Tech Research Institute ..... Atlanta, GA
Implemented prototype system for single sign-on for Department of Justice web applications used in the JFed project.

2002-2004 **Research Assistant**, College of Computing, Georgia Tech ..... Atlanta, GA

Summer 2003 **Teaching Assistant**, Universitat Polytèchnica de Catalunya ..... Barcelona, Spain

2000-2002 **IT Systems Manager**, Tinder Wholesale ..... Manassas, VA
Led development and deployment team for company's first e-commerce system.

1998-2000 **Developer and System Administrator**, Tinder Wholesale ..... Manassas, VA

1997-2002 **Founder**, Cytech Web Development ..... Chantilly, VA
Founded and ran company that provided web application development and web hosting.

Summer 1997 **Intern**, U.S. Geological Survey ..... Reston, VA
Designed and developed prototype web application to sell USGS maps.

Teaching Experience

Spring 2008 **Guest Lecturer.** Introduction to Software Engineering (CS 3300), Georgia Tech

Spring 2006 **Guest Lecturer.** Introduction to Database Systems (CS 4400), Georgia Tech

Spring 2005 **Guest Lecturer.** Introduction to Software Engineering (CS 3300), Georgia Tech

Summer 2003 **Teaching Assistant.** Universitat Polytèchnica de Catalunya

Developed course materials, graded, and taught majority of classes for undergraduate software engineering class.

Professional Activities

2008-2009 **Journal Reviewer:** Journal on Software Testing, Verification and Reliability. Editor: Paul Ammann; Journal of Systems and Software. Editor: Antonia Bertolino.

2005-2008 **Conference Reviewer:** FSE 2008, FSE 2007, ASE 2005.

2006-2007 **Graduate Student Council:** Member of travel sub-committee. Developed and administered policy for allocating student travel funding.

Awards

2009 **ACM Distinguished Paper Award:** Awarded at the International Symposium on Software Testing and Analysis, Chicago, IL.

2009 **Best Presentation:** Award for best presentation at the International Conference on Software Testing, Denver, CO.

2008 **Best Student Presentation:** Award for best student presentation at Foundations of Software Engineering, Atlanta, GA.

2005-2009 **Goizueta Foundation Fellowship:** Awarded to graduate students of Hispanic/Latino origin who demonstrate exemplary levels of scholarship and innovation in their academic departments.

2004-2005 **Shackelford Fellow:** Fellowship program to promote collaboration between the Georgia Tech Research Institute and academic units of Georgia Tech.

2003 **Verizon Foundation Fellowship:** In recognition of outstanding academic performance.

1998-2002 **IBM/NACME Scholar:** Scholarship program to support leadership and academic development for minority students in science, engineering, technology, and math based educational fields.

Patents

2007 **"Data-driven Profiling for Distributed Web 2.0 Applications,"** patent applied for technology and techniques developed during summer of 2007 at Microsoft.

Tools and Infrastructure

WAIVE: Verify interactions between components of a web application. This tool performs a static analysis of a web application in order to identify invocations generated by the application. WAIVE then verifies the invocations against the set of interfaces identified by the WAM tool. Available on request.

WAM: Identify web application interfaces. This tool performs a static analysis of a web application in order to identify the parameters that comprise the application's interfaces and domain constraints on the parameters. Available on request.

SQL Injection Testbed: Testbed of vulnerable web applications along with corresponding test datasets that include legitimate accesses and SQL injection attacks. The testbed is available via my website and has been distributed to over twenty universities and research labs.

WASP: Protect web applications from SQL injection attacks. WASP uses positive tainting, which identifies and marks trusted strings in a web application, and syntax-aware evaluation, which controls the usage of strings in database queries based on their trust markings and syntactic position. WASP also uses MetaStrings, a library that I developed to track taint information at the character level. Currently, WASP is in commercialization.

DITTO: Measure command-form coverage of a test suite. This tool identifies testing requirements based on the command-form coverage criterion and and monitors coverage of the criterion during testing. DITTO is available on request and has been distributed to several university-based researchers.

AMNESIA: Protect web applications from SQL injection attacks. This tool uses a conservative static analysis to build a model of the legitimate queries that can be generated by a web application. At runtime, it checks that each query complies with the model. AMNESIA is available via my website and has been distributed to over forty universities and research labs.

Other Contributions

2007 **WASP Commercialization:** Worked with Reflective Inc. to commercialize the WASP tool.

2005 **HSARPA Funding:** Participated in writing grant proposal that led to funding of grant FA8750-05-2-0214.

Professional Affiliation

- Association of Computing Machinery (ACM), Member.
- ACM Special Interest Group on Software Engineering (SIGSOFT), Member.
- Institute of Electrical and Electronics Engineers (IEEE), Member.
- Society of Hispanic Professional Engineers (SHPE), Member.

Personal Information

U.S. citizen. Fluent in Spanish, oral and written.