

WILLIAM ROBERTSON, PH.D.

CONTACT INFORMATION

731 Soda Hall
Computer Science Division
University of California, Berkeley
Berkeley, CA 94720-1776 USA

Voice: +1 (805) 895-1407
Work: +1 (805) 893-4394
E-mail: wkr@eecs.berkeley.edu
WWW: <http://wilrobertson.com/>

RESEARCH INTERESTS

My primary research interest is in protecting web applications from attacks. One line of research has focused on using statistical machine learning techniques to automatically construct models characterizing the normal behavior of web applications in order to perform accurate, black-box anomaly detection of web-based attacks. Recent work in this area has focused on addressing fundamental challenges to performing web application anomaly detection, such as reducing the rate of false positives, adapting to changes in web application behavior over time, and compensating for the scarcity of training data. Another approach I am investigating is the construction of development frameworks to build web applications that are automatically secure against certain classes of attacks by construction.

Other research interests include intrusion detection system testing and evasion, electronic voting security, and the verification of software security properties using static and dynamic analysis techniques.

EDUCATION

University of California, Santa Barbara
Ph.D., Computer Science

June 2003 – June 2009
Santa Barbara, CA USA

- Advised by Professors Dick Kemmerer and Giovanni Vigna
- Thesis entitled “Detection and Prevention of Web-based Attacks”

University of California, Santa Barbara
B.S., Computer Science

September 1997 – June 2002
Santa Barbara, CA USA

ACADEMIC EXPERIENCE

University of California, Berkeley
Postdoctoral Researcher

October 2009 – Present
Berkeley, CA USA

- Member of Professor David Wagner’s computer security research group

University of California, Santa Barbara
Research Assistant, Computer Security Group

June 2002 – September 2009
Santa Barbara, CA USA

- Member of Ohio Evaluation and Validation of Election-Related Equipment, Standards, and Testing (EVEREST) Red Team (ES&S system)
- Member of California Top-To-Bottom Electronic Voting Systems Review (TTBR) Red Team (Sequoia system)

TEACHING EXPERIENCE

University of California, Santa Barbara
Guest lecturer

September 2003 – September 2007
Santa Barbara, CA USA

- Guest lecturer for introductory computer security course
- Guest lecturer for graduate computer security course

**PROFESSIONAL
EXPERIENCE**

WebWise Security, Inc.
CTO, Co-Founder

September 2006 – October 2008
Santa Barbara, CA USA

- Co-founded, along with advisors, web application security company focused on providing solutions for designing, auditing, and protecting web-based applications and services
- Co-developer of *weblock*, a high-speed anomaly-based web application firewall (WAF) designed to detect and prevent both known and unknown attacks against custom web-based applications and services

Sun Microsystems, Inc.
Intern

June 1998 – September 2001
Mountain View, CA USA

- Designed and implemented a testing framework for system controllers deployed in the Serengeti enterprise server platform in conjunction with the Performance Application Engineering (PAE) group

**PROFESSIONAL
SERVICE**

Program Committee member for the 2010 OWASP AppSec Europe Conference

Program Committee member for the 2010 International Conference on Distributed Computing Systems (ICDCS), Security Track

Program Committee member for the 2010 International Workshop on Software Engineering for Secure Systems, co-located with the International Conference on Software Engineering (ICSE)

Program Committee member for the 2010 European Workshop on System Security (EuroSec), co-located with the 2010 EuroSys Conference

**JOURNAL
PUBLICATIONS**

D. Balzarotti, M. Cova, V. Felmetsger, R. Kemmerer, W. Robertson, F. Valeur, G. Vigna. An Experience in Testing the Security of Real-World Electronic Voting Systems. *IEEE Transactions on Software Engineering*, 2010.

G. Vigna, F. Valeur, D. Balzarotti, W. Robertson, C. Kruegel, E. Kirda. Reducing Errors in the Anomaly-based Detection of Web-based Attacks Through the Combined Analysis of Web Requests and SQL Queries. *Journal of Computer Security*, 17(3), May 2009.

C. Kruegel, G. Vigna, and W. Robertson. A Multi-model Approach to the Detection of Web-based Attacks. *Journal of Computer Networks*, 48(5):717–738, July 2005.

C. Kruegel, W. Robertson, and G. Vigna. Using Alert Verification to Identify Successful Intrusion Attempts. *Journal of Practice in Information Processing and Communication (PIK)*, 27(4), August 2004.

**CONFERENCE
PUBLICATIONS**

F. Maggi, W. Robertson, C. Kruegel, G. Vigna. Protecting a Moving Target: Addressing Web Application Concept Drift. In *Proceedings of the International Symposium on Recent Advances in Intrusion Detection (RAID)*, Saint-Malo, Brittany, FR, September 2009.

W. Robertson, G. Vigna. Static Enforcement of Web Application Integrity Through Strong Typing. In *Proceedings of the USENIX Security Symposium*, Montreal, QC, CA, August 2009.

D. Balzarotti, G. Banks, M. Cova, V. Felmetsger, R. A. Kemmerer, W. Robertson, F. Valeur, and G. Vigna. Are Your Votes Really Counted? Testing the Security of Real-world Electronic Voting Systems. In *Proceedings of the International Symposium on Software Testing and Analysis (ISSTA 2008)*, Seattle, WA, USA, July 2008.

D. Balzarotti, W. Robertson, C. Kruegel, and G. Vigna. Improving Signature Testing Through Dynamic Data Flow Analysis. In *Proceedings of the 23rd Annual Computer Security Applications Conference (ACSAC)*, Miami Beach, FL, USA, December 2007.

D. Mutz, W. Robertson, G. Vigna, and R. A. Kemmerer. Exploiting Execution Context for the Detection of Anomalous System Calls. In *Proceedings of the 10th International Symposium on Recent Advances in Intrusion Detection (RAID)*, Gold Coast, Queensland, AU, September 2007.

W. Robertson, G. Vigna, C. Kruegel, and R. A. Kemmerer. Using Generalization and Characterization Techniques in the Anomaly-based Detection of Web Attacks. In *Proceedings of the 13th Annual Network and Distributed System Security Symposium (NDSS)*, San Diego, CA, USA, February 2006.

C. Kruegel, E. Kirda, D. Mutz, W. Robertson, and G. Vigna. Polymorphic Worm Detection Using Structural Information of Executables. In *Proceedings of the 8th International Symposium on Recent Advances in Intrusion Detection (RAID)*, Seattle, WA, USA, September 2005.

C. Kruegel, E. Kirda, D. Mutz, W. Robertson, and G. Vigna. Automating Mimicry Attacks Using Static Binary Analysis. In *Proceedings of the 14th USENIX Security Symposium*, Baltimore, MD, USA, July 2005.

D. Mutz, C. Kruegel, W. Robertson, G. Vigna, and R. A. Kemmerer. Reverse Engineering of Network Signatures. In *Proceedings of the 4th Annual Asia Pacific Information Technology Security Conference (AusCERT)*, Gold Coast, Queensland, AU, May 2005.
Received Best Paper Award.

C. Kruegel, W. Robertson, and G. Vigna. Detecting Kernel-Level Rootkits Through Binary Analysis. In *Proceedings of the 20th Annual Computer Security Applications Conference (ACSAC)*, Tuscon, AZ, USA, December 2004.

G. Vigna, W. Robertson, and D. Balzarotti. Testing Network-based Intrusion Detection Signatures Using Mutant Exploits. In *Proceedings of the 11th ACM Conference on Computer and Communications Security (CCS)*, Washington DC, USA, October 2004.

C. Kruegel, W. Robertson, F. Valeur, and G. Vigna. Static Disassembly of Obfuscated Binaries. In *Proceedings of the 13th USENIX Security Symposium*, San Diego, CA, USA, August 2004.

G. Vigna, W. Robertson, V. Kher, and R. A. Kemmerer. A Stateful Intrusion Detection System for World-Wide Web Servers. In *Proceedings of the 19th Annual Computer Security Applications Conference (ACSAC)*, Las Vegas, NV, USA, December 2003.

C. Kruegel, D. Mutz, W. Robertson, and F. Valeur. Bayesian Event Classification for Intrusion Detection. In *Proceedings of the 19th Annual Computer Security Applications Conference (ACSAC)*, Las Vegas, NV, USA, December 2003.

W. Robertson, C. Kruegel, D. Mutz, and F. Valeur. Run-time Detection of Heap-based Overflows. In *Proceedings of the 17th USENIX Large Installation Systems Administration Conference (LISA)*, San Diego, CA, USA, October 2003.

C. Kruegel, D. Mutz, W. Robertson, and F. Valeur. Topology-based Detection of Anomalous BGP Messages. In *Proceedings of the 6th International Symposium on Recent Advances in Intrusion Detection (RAID)*, Pittsburgh, PA, USA, September 2003.

**WORKSHOP
PUBLICATIONS**

C. Kruegel and W. Robertson. Alert Verification: Determining the Success of Intrusion Attempts. In *Proceedings of the 1st Workshop on the Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA)*, Dortmund, GER, July 2004.

**PROFESSIONAL
AFFILIATIONS**

IEEE Computer Society
Association for Computing Machinery
USENIX Association

REFERENCES

Professor Richard A. Kemmerer
2165 Engineering I
Department of Computer Science
University of California, Santa Barbara
Santa Barbara, CA 93106-5110
United States
+1 (805) 893-4232
kemm@cs.ucsb.edu

Professor Christopher Kruegel
1117 Engineering I
Department of Computer Science
University of California, Santa Barbara
Santa Barbara, CA 93106-5110
United States
+1 (805) 893-6198
chris@cs.ucsb.edu

Professor Wenke Lee
3142 Klaus Advanced Computing
Georgia Institute of Technology
266 Ferst Drive
Atlanta, GA 30332-0765
United States
+1 (404) 385-2879
wenke@cc.gatech.edu

Professor Giovanni Vigna
2159 Engineering I
Department of Computer Science
University of California, Santa Barbara
Santa Barbara, CA 93106-5110
United States
+1 (805) 893-7565
vigna@cs.ucsb.edu

Professor Engin Kirda
Graduate School and Research Center
Institut Eurecom
2229 Route des Cretes
F-06560 Sophia-Antipolis cedex
France
+33 4 9300 8247
kirda@eurecom.fr

Professor Matt Bishop
3059 John D. Kemper Hall
Department of Computer Science
University of California, Davis
One Shields Ave
Davis, CA 95616-8562
United States
+1 (530) 752-8060
bishop@cs.ucdavis.edu

CITIZENSHIP

United States