William Kim Robertson

Contact Information

2114 Engineering I
Department of Computer Science
UC Santa Barbara
Santa Barbara, CA 93106-5110 USA

Voice:	+1-805-895-1407
Work:	+1-805-893-4394
E-mail:	wkr@cs.ucsb.edu
WWW:	http://www.cs.ucsb.edu/˜wkr/

Research Interests

My current research interests include signature and anomaly-based intrusion detection of the network, host, and application domains. In particular, recent work has focused on the integration of traditional signature-based detection with novel methods for the efficient construction and evaluation of positive anomaly-based models to detect and prevent attacks against web-based applications and web services.

Other research interests include the static and dynamic analysis of binary code, system languages, and scripting languages to detect security vulnerabilities against critical applications and services.

Academic Experience

University of California, Santa Barbara — **June 2002 - Present**
Ph.D. Student, Computer Science — Santa Barbara, CA USA

- Research assistant working with Professors Dick Kemmerer and Giovanni Vigna in the UCSB Computer Security Group
- Member of team that won the 2005 DEFCON Capture the Flag, an internationally-recognized computer hacking competition
- Performed extensive research into application-level anomaly detection
- Performed extensive research into multi-domain signature-based intrusion detection of multiple event streams
- Researched and designed heap overflow prevention system subsequently integrated into GNU libc, now deployed on all modern Linux-based systems
- Participated in multiple technology transfers to funding agencies
- Performed research into various areas of computer security, including polymorphic worm detection, signature and anomaly-based IDS testing and evasion, static and dynamic analysis of user and kernel-level code, and the detection of attacks against the global routing infrastructure

University of California, Santa Barbara — **September 1997 - June 2002**
B.S, Computer Science — Santa Barbara, CA USA

Professional Experience

WebWise Security, Inc. — **September 2006 - Present**
CTO, Co-Founder — Santa Barbara, CA USA

- Co-founded 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
- Co-inventor of patent-pending *anomaly signature* technology to cluster and characterize sets of anomalies to both dramatically reduce false positive rates as well as identify representative attacks

- Provides black and gray-box system and network penetration testing services, white-box code auditing and analysis, and security training courses

Sun Microsystems, Inc. **June 1998 - September 2001**
Intern Mountain View, CA USA

- Collaborated with Performance Application Engineering (PAE) group to design and implement a testing framework for system controllers deployed in the Serengeti enterprise server platform

Journal Publications

"A Multi-model Aproach to the Detection of Web-based Attacks"
C. Kruegel, G. Vigna, W. Robertson.
In the Journal of Computer Networks.
Vol. 48, No. 5, July 2005.

"Using Alert Verification to Identify Successful Intrusion Attempts"
C. Kruegel, W. Robertson, G. Vigna.
In the Journal of Practice in Information Processing and Communication (PIK).
Vol. 27, No. 4, October 2004.

Conference Publications

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

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

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

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

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

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

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

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

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

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

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

Workshop Publications

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