William Robertson, Ph.D.

Contact Information

360 Huntington Ave
College of Computer and Information Science
Northeastern University
Boston, MA 02115-5000

Voice: +1 (617) 373-2136
E-mail: wkr@ccs.neu.edu
Web: https://wkr.io/

Education

University of California, Santa Barbara — **June 2003 – June 2009**
Ph.D., Computer Science — Santa Barbara, CA, USA

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

Academic Experience

Northeastern University — **September 2017 – Present**
Associate Professor — Boston, MA, USA

Northeastern University — **September 2011 – August 2017**
Assistant Professor — Boston, MA, USA

University of California, Berkeley — **October 2009 – August 2011**
Postdoctoral Researcher — Berkeley, CA, USA

University of California, Santa Barbara — **June 2002 – September 2009**
Research Assistant, Computer Security Group — Santa Barbara, CA, USA

Professional Experience

Lastline, Inc. — **June 2013 – Present**
Consultant — Santa Barbara, CA, USA

WebWise Security, Inc. — **September 2006 – October 2008**
CTO, Co-Founder — Santa Barbara, CA, USA

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

Professional Service

Program Committee Chair

- Annual Computer Security Applications Conference (ACSAC 2015–2016)
- USENIX Workshop on Offensive Technologies (WOOT 2013)
- International Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA 2012)

Program Committee Member

- IEEE Symposium on Security and Privacy (Oakland 2011–2013, 2015, 2019)
- ACM Conference on Computer and Communications Security (CCS 2015–2017, 2018–2019)
- USENIX Security Symposium (2011, 2015–2017)
- ISOC Network and Distributed System Symposium (NDSS 2015, 2017)
- Applied Computer Security Applications Conference (ACSAC 2014)
- Other top-tier security conferences and workshops

Journal Reviewer

- IEEE Transactions on Dependable and Secure Computing (TDSC)

- ACM Transactions on Information and System Security (TISSEC)
- IEEE Transactions on Knowledge and Data Engineering (TKDE)
- IEEE Transactions on Software Engineering (TSE)
- IEEE Transactions on Computers (TC)
- Other top-tier security journals

Professional Memberships

- Association of Computing Machinery (ACM)
- IEEE Computer Society
- USENIX Association

Projects

- Plasticity: Breaking the Vicious Crash-Recover Cycle for Brittle Firmware (ONR)
- Continuum: Finding Space and Time Vulnerabilities in Java Programs (DARPA)
- Automated Reverse Engineering of Commodity Software (NSF)
- Firmalice: Modifying and Identifying Malice in Firmware (DARPA)
- Automated Inference of Binary Program Structure (ONR)
- DarkDroid: Exposing the Dark Side of Android Marketplaces (DARPA)
- Multi-Disciplinary Preparation of Next Generation Information Assurance Practitioners (NSF)

Conference Publications

T. Lauinger, A. Buyukkayhan, A. Chaabane, W. Robertson, E. Kirda. From Deletion to Re-Registration in Zero Seconds: Domain Registrar Behavior During the Drop. To appear in *Proceedings of the ACM Internet Measurement Conference (IMC)*. Boston, MA, November 2018.

M. A. Bashir, S. Arshad, E. Kirda, W. Robertson, C. Wilson. How Tracking Companies Circumvented Ad Blockers Using WebSockets. To appear in *Proceedings of the ACM Internet Measurement Conference (IMC)*. Boston, MA, November 2018.

A. Kharraz, W. Robertson, E. Kirda. Surveylance: Automatically Detecting Online Survey Scams. In *Proceedings of the IEEE Symposium on Security and Privacy (Oakland)*. San Francisco, CA, May 2018.

K. Onarlioglu, W. Robertson, E. Kirda. ERASER: Your Data Won't Be Back. In *Proceedings of the IEEE European Symposium on Security and Privacy (EUROSP)*. London, UK, April 2018.

S. Arshad, S. Mirheidari, T. Lauinger, B. Crispo, E. Kirda, W. Robertson. Large-Scale Analysis of Style Injection by Relative Path Overwrite. In *Proceedings of the Web Conference (WWW)*. Lyon, FR, April 2018.

M. Weissbacher, E. Mariconti, G. Suarez de Tangil, W. Robertson, E. Kirda. Ex-Ray: Detection of History-Leaking Browser Extensions. In *Proceedings of the Annual Computer Security Applications Conference (ACSAC)*. Puerto Rico, USA, December 2017.

A. Buyukkayhan, A. Oprea, Z. Li, W. Robertson. Lens on the Endpoint: Hunting for Malicious Software through Endpoint Data Analysis. In *Proceedings of the International Symposium on Research in Attacks, Intrusions, and Defenses (RAID)*. Atlanta, GA, USA, September 2017.

T. Lauinger, A. Chaabane, A. Buyukkayhan, K. Onarlioglu, W. Robertson. Game of Registrars: An Empirical Analysis of Post-Expiration Domain Name Takeovers. In *Proceedings of the USENIX Security Symposium*. Vancouver, BC, CA, August 2017.

W. Koch, A. Chaabane, M. Egele, W. Robertson, E. Kirda. Semi-Automated Discovery of Server-Based Information Oversharing Vulnerabilities in Android Applications. In *Proceedings of the International Symposium on Software Testing and Analysis (ISSTA)*. Santa Barbara, CA, USA, July 2017.

T. Lauinger, A. Chaabane, W. Robertson, C. Wilson, E. Kirda. Thou Shalt Not Depend on Me: Analysing the Use of Outdated JavaScript Libraries on the Web. In *Proceedings of the ISOC Network and Distributed Security Symposium (NDSS)*. San Diego, CA, USA, February 2017.

T. Lauinger, K. Onarlioglu, A. Chaabane, W. Robertson, E. Kirda. WHOIS Lost in Translation: (Mis)Understanding Internet Domain Name Expiration and Re-Registration. In *Proceedings of the ACM Internet Measurement Conference (IMC)*. Santa Monica, CA, USA, November 2016.

S. Arshad, A. Kharraz, W. Robertson. Identifying Extension-based Ad Injection via Fine-grained Web Content Provenance. In *Proceedings of the International Symposium on Research in Attacks, Intrusions, and Defenses (RAID)*. Paris, FR, September 2016.

A. Mambretti, K. Onarlioglu, C. Mulliner, W. Robertson, E. Kirda, F. Maggi, S. Zanero. Trellis: Privilege Separation for Multi-User Applications Made Easy. In *Proceedings of the International Symposium on Research in Attacks, Intrusions, and Defenses (RAID)*. Paris, FR, September 2016.

M. Bashir, S. Arshad, W. Robertson, C. Wilson. Tracing Information Flows Between Ad Exchanges Using Retargeted Ads. In *Proceedings of the USENIX Security Symposium*. Austin, TX, USA, August 2016.

A. Kharraz, S. Arshad, C. Mulliner, W. Robertson, E. Kirda. UNVEIL: A Large-Scale, Automated Approach to Detecting Ransomware. In *Proceedings of the USENIX Security Symposium*. Austin, TX, USA, August 2016.

S. Duman, K. Kalkan, M. Egele, W. Robertson, E. Kirda. EmailProfiler: Spearphishing Filtering with Header and Stylometric Features of Emails. In *Proceedings of the IEEE Computer Society International Conference on Computers, Software & Applications (COMPSAC)*. Atlanta, GA, USA, June 2016.

K. Onarlioglu, W. Robertson, E. Kirda. Overhaul: Input-Driven Access Control for Better Privacy on Traditional Operating Systems. In *Proceedings of the IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*. Toulouse, FR, June 2016.

Y. Fratantonio, A. Bianchi, W. Robertson, C. Kruegel, E. Kirda, G. Vigna. Towards Detecting Logic Bombs in Android Applications. In *Proceedings of the IEEE Symposium on Security and Privacy (Oakland)*. San Jose, CA, USA, May 2016.

B. Dolan-Gavitt, P. Hulin, E. Kirda, T. Leek, A. Mambretti, W. Robertson, F. Ulrich, R. Whelan. LAVA: Large-scale Automated Vulnerability Addition. In *Proceedings of the IEEE Symposium on Security and Privacy (Oakland)*. San Jose, CA, USA, May 2016.

P. Carter, C. Mulliner, M. Lindorfer, W. Robertson, E. Kirda. CuriousDroid: Automated User Interface Interaction for Android Application Analysis Sandboxes. In *Proceedings of the International Conference on Financial Cryptography and Data Security (FC)*. Barbados, February 2016.

S. Arshad, A. Kharraz, W. Robertson. Include Me Out: In-Browser Detection of Malicious Third-Party Content Inclusions. In *Proceedings of the International Conference on Financial Cryptography and Data Security (FC)*. Barbados, February 2016.

A. Buyukkayhan, K. Onarlioglu, W. Robertson, E. Kirda. CrossFire: An Analysis of Firefox

Extension-Reuse Vulnerabilities. In *Proceedings of the Network and Distributed System Security Symposium (NDSS)*. San Diego, CA, USA, February 2016.

M. Weissbacher, W. Robertson, E. Kirda, C. Kruegel, G. Vigna. ZigZag: Automatically Hardening Web Applications Against Client-side Validation Vulnerabilities. In *Proceedings of the USENIX Security Symposium*. Washington DC, USA, August 2015.

Y. Fratantonio, A. Bianchi, W. Robertson, M. Egele, E. Kirda, C. Kruegel, G. Vigna. On the Security and Engineering Implications of Finer-Grained Access Controls for Android Developers and Users. In *Proceedings of the International Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA)*. Milan, IT, July 2015.

A. Kharraz, W. Robertson, D. Balzarotti, L. Bilge, E. Kirda. Cutting the Gordian Knot: A Look Under the Hood of Ransomware Attacks. In *Proceedings of the International Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA)*. Milan, IT, July 2015.

A. Ozcan, C. Gemicioglu, K. Onarlioglu, M. Weissbacher, C. Mulliner, W. Robertson, E. Kirda. BabelCrypt: The Universal Encryption Layer for Mobile Messaging Applications. In *Proceedings of the International Conference on Financial Cryptography and Data Security (FC)*. Isla Verde, PR, USA, January 2015.

S. Duman, K. Onarlioglu, A. Ulosoy, W. Robertson, E. Kirda. TrueClick: Automatically Distinguishing Trick Banners from Genuine Download Links. In *Proceedings of the Annual Computer Security Applications Conference (ACSAC)*. New Orleans, LA, USA, December 2014.

M. Weissbacher, T. Lauinger, W. Robertson. Has CSP Failed? A Large-Scale Evaluation of the Feasibility of CSP Adoption. In *Proceedings of the International Symposium on Research in Attacks, Intrusions, and Defenses (RAID)*. Gothenburg, SE, September 2014.

A. Kharraz, E. Kirda, W. Robertson, D. Balzarotti, A. Francillon. Optical Delusions: A Study of Malicious QR Codes in the Wild. In *Proceedings of the IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*. Atlanta, GA, USA, June 2014.

C. Mulliner, W. Robertson, E. Kirda. VirtualSwindle: An Automated Attack Against In-App Billing on Android. In *Proceedings of the ACM Symposium on Information, Computer, and Communications Security (ASIACCS)*. Kyoto, JP, June 2014.

C. Mulliner, W. Robertson, E. Kirda. Hidden GEMs: Automated Discovery of Access Control Vulnerabilities in Graphical User Interfaces. In *Proceedings of the IEEE Symposium on Security and Privacy (Oakland)*. San Jose, CA, USA, May 2014.

T.-F. Yen, A. Oprea, K. Onarlioglu, T. Leetham, W. Robertson, A. Juels, E. Kirda. Beehive: Large-Scale Log Analysis for Detecting Suspicious Activity in Enterprise Networks. In *Proceedings of the Annual Computer Security Applications Conference (ACSAC)*. New Orleans, LA, USA, December 2013.

C. Mulliner, J. Oberheide, W. Robertson, E. Kirda. PatchDroid: Scalable Third-Party Patches for Android Devices. In *Proceedings of the Annual Computer Security Applications Conference (ACSAC)*. New Orleans, LA, USA, December 2013.

T. Lauinger, K. Onarlioglu, A. Chaabane, E. Kirda, W. Robertson, M. Kaafar. Holiday Pictures or Blockbuster Movies? Insights into Copyright Infringement in User Uploads to One-Click File Hosters. In *Proceedings of the International Symposium on Research in Attacks, Intrusions, and Defenses (RAID)*. St. Lucia, LC, October 2013.

K. Onarlioglu, M. Battal, W. Robertson, E. Kirda. Securing Legacy Firefox Extensions with

Sentinel. In *Proceedings of the International Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA)*. Berlin, DE, July 2013.

K. Onarlioglu, C. Mulliner, W. Robertson, E. Kirda. PrivExec: Private Execution as an Operating System Service. In *Proceedings of the IEEE Symposium on Security and Privacy*, San Francisco, CA, USA, May 2013.

A. Cassola, W. Robertson, E. Kirda, G. Noubir. A Practical, Targeted, and Stealthy Attack Against WPA Enterprise Authentication. In *Proceedings of the Network and Distributed System Security Symposium (NDSS)*, San Diego, CA, USA, February 2013.

E. Blass, W. Robertson. Tresor-Hunt: Attacking CPU-Bound Encryption. In *Proceedings of the Annual Computer Security Applications Conference (ACSAC)*, Orlando, FL, USA, December 2012.

L. Bilge, D. Balzarotti, W. Robertson, E. Kirda, C. Kruegel. Disclosure: Detecting Botnet Command and Control Servers Through Large-Scale NetFlow Analysis. In *Proceedings of the Annual Computer Security Applications Conference (ACSAC)*, Orlando, FL, USA, December 2012.

T. Scholte, W. Robertson, D. Balzarotti, E. Kirda. Preventing Input Validation Vulnerabilities in Web Applications through Automated Type Analysis. In *Proceedings of the IEEE Computer Society International Conference on Computers, Software & Applications (COMPSAC)*. Izmir, TK, July 2012.

T. Scholte, D. Balzarotti, W. Robertson, E. Kirda. An Empirical Analysis of Input Validation Mechanisms in Web Applications and Languages. In *Proceedings of the ACM Symposium on Applied Computing (SAC)*, Trento, IT, March 2012.

W. Robertson, F. Maggi, C. Kruegel, G. Vigna. Effective Anomaly Detection with Scarce Training Data. In *Proceedings of the Network and Distributed System Security Symposium (NDSS)*, San Diego, CA, USA, February 2010.

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, 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, G. Vigna. Improving Signature Testing Through Dynamic Data Flow Analysis. In *Proceedings of the Annual Computer Security Applications Conference (ACSAC)*, Miami Beach, FL, USA, December 2007.

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

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

2006.

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

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

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

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

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

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

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

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

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

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

Journal Publications

K. Onarlioglu, A. Buyukkayhan, W. Robertson, E. Kirda. Sentinel: Securing Legacy Firefox Extensions. *Computers and Security*, 49(0), January 2015.

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*, 36(4), August 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, 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, G. Vigna. Using Alert Verification to Identify Successful Intrusion Attempts. *Journal of Practice in Information Processing and Communication (PIK)*, 27(4), August 2004.

Workshop Publications

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

Invited Talks

A Game of Registrars: The Shaky Foundations of Domain-based Security
Royal Holloway University of London, September 2017

Systems Security Research
National University of Singapore, August 2017

TriggerScope: Detecting Malicious Functionality without Application Specifications
Rensselaer Polytechnic Institute, May 2017

TriggerScope: Detecting Malicious Functionality without Application Specifications
MIT/LL CORE Series, May 2016

CrossFire: An Analysis of Firefox Extension-Reuse Vulnerabilities
BlackHat Asia, March 2016

How to Get Away with Malware (and, How to Catch an Attacker)
Stony Brook University, March 2016

How to Get Away with Malware (and, How to Catch an Attacker)
Chalmers University, February 2016

Whither Systems Security?
New England Security Day, September 2015

Systems Security Research
United States Secret Service Workshop, March 2015

Attacking Graphical User Interfaces
Yokohama National University, March 2015

Future Directions in Defending Industrial Control Systems
ONR Industrial Control Systems Security Workshop, January 2015

Congressional Briefing on Cybersecurity
Capitol Hill, Washington DC, November 2013

Memory Corruption Attacks
MITLL CTF Seminar, November 2013

PrivExec: Private Execution as an Operating System Service
MIT Security Seminar, October 2013.

Divining Intent: Exposing Hidden Malicious Functionality on Android Devices
ACM ESWEEK/WESS Keynote, September 2013.

NU Systems Security Overview
NYU Poly, May 2013

Memory Corruption Attacks
MITLL CTF Seminar, November 2012

Capture-the-Flag
NU/MITLL Seminar, March 2012

Large-scale, Wide-area Botnet Detection
Symantec Research Labs, January 2012

Recent Directions in Web Application Security
UMass Lowell, November 2011

Web Application Anomaly Detection in a Web 2.0 World.
Schloss Dagstuhl – Leibniz Center for Informatics, April 2009.

Citizenship United States