William Robertson

🏢 177 Huntington Ave, Office 614, Boston MA, 02115
✉ w.robertson@northeastern.edu — 🌐 wkr.io

Education

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

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

Academic Appointments

Northeastern University Boston, MA
Associate Professor September 2017 — Present

Yokohama National University Yokohama, JP
Visiting Associate Professor March 2019 — March 2021

Yokohama National University Yokohama, JP
Visiting Assistant Professor March 2014 — March 2019

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

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

University of California, Santa Barbara Santa Barbara, CA
Graduate Research Assistant June 2002 — September 2009

Professional Experience

Lastline, Inc. Santa Barbara, CA
Consultant, Android Malware Analysis June 2013 — June 2020

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

Sun Microsystems, Inc. Mountain View, CA
Intern, Performance Application Engineering June 1998 — September 2001

Research Supervision

Current Ph.D. Students	**Research Topic**	**Date**
Kai Bernardini	Malware Detection	Spring 2028
Cassidy Waldrip	Software Testing	Spring 2028
Xenia Dragon	Side Channel Analysis	Spring 2027
Genoveva Fossas	Software Hardening	Spring 2026

Research Scientists and Postdocs	**Institution**	**Position**	**Date**
Ioannis Agadakos	Amazon Web Services	Research Scientist	Spring 2023
Jeremiah Onaolapo	University of Vermont	Assistant Professor	Spring 2020
Abdelberi Chaabane	INRIA	Research Scientist	Spring 2017

Collin Mulliner	Cruise	Security Architect	Spring 2016

Graduated Ph.D. Students	**Institution**	**Position**	**Date**
Andrew Fasano	MIT Lincoln Laboratory	Research Scientist	Spring 2024
Joshua Bundt	West Point Army Cyber Institute	Research Scientist	Spring 2023
Ahmet Buyukkayhan	Microsoft	Security Engineer	Spring 2019
Sajjad Arshad	Google	Security Engineer	Spring 2019
Michael Weissbacher	Block (formerly Square)	Security Engineer	Spring 2018
Tobias Lauinger	New York University	Postdoc	Fall 2018
Amin Kharraz	Florida International University	Assistant Professor	Fall 2017
Sevtap Duman	Ege University	Assistant Professor	Summer 2017
Kaan Onarlioglu	Akamai	Security Engineer	Fall 2016

M.S. Students	**Research Topic**	**Date**
Devin Quinn	Misinformation Detection using Large Language Models	Fall 2023
Leo St. Amour	Interactive Synthesis of Software Security Policies	Spring 2017
Patrick Carter	Testing Android Application User Interfaces	Spring 2016
Brandon Daley	USB Attack Anomaly Detection	Spring 2016
Francis Adkins	Maximizing Test Coverage for Binary Programs	Spring 2015
Louis Bloom	Program Partitioning	Spring 2014
Ryan Rickert	Dynamic Invariant Detection on Binary Programs	Spring 2013

Funded Research Projects

Securing the Future: Scholarship for Service at Northeastern University	NSF	PI
Making Security Work: Vulnerability Disclosure Programs and the Organizational Foundations of Security	NSF	Co-PI
DoD CySP at Northeastern University	NSA	Co-PI
Automated Low-Latency Breach Mitigation	Infradata	Co-PI
In-Situ Malware Containment and Deception through Dynamic In-Process Virtualization	ONR	Co-PI
Google Security and Privacy Award: Cloud Security	Google	Co-PI
Taming Memory Corruption with Security Monitors	NSF	Co-PI
A Bug's Life: An Ethnography of a Flaw	NSF	Co-PI
Defending Cyber-Physical Systems using Federated Learning of Physical Models	ONR	Co-PI
Plasticity: Breaking the Vicious Crash-Recover Cycle for Brittle Firmware	ONR	Co-PI
Continuum: Finding Space and Time Vulnerabilities in Java Programs	DARPA	PI
Firmalice: Modifying and Identifying Malice in Firmware	DARPA	Co-PI
Automated Reverse Engineering of Commodity Software	NSF	Co-PI
Multi-Disciplinary Preparation of Next Generation Information Assurance Practitioners	NSF	Co-PI
LAVA: Lincoln Application Vulnerability Automation	MITLL	PI
Automated Inference of High-Level Program Structure	ONR	PI
DarkDroid: Exposing the Dark Side of Android Marketplaces	DARPA	Co-PI

Selected Professional Service

IEEE Symposium on Security and Privacy	*Associate Chair*	2025
	PC Member	2011–2013, 2015, 2019–2021, 2023–2024
USENIX Security Symposium	PC Member	2011, 2015–2017, 2021–2022
ACM Conference on Computer and Communications Security (CCS)	PC Member	2015–2017, 2018–2020
ISOC Network and Distributed System Security Symposium (NDSS)	PC Member	2015, 2017, 2023, 2025
Annual Computer Security Applications Conference (ACSAC)	*Program Chair*	2015–2016
	Test of Time Award Chair	2023–2024
USENIX Workshop on Offensive Technologies (WOOT)	*Program Chair*	2013
International Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA)	*Program Chair*	2012

Selected Publications

Joshua Bundt, Michael Davinroy, Ioannis Agadakos, Alina Oprea, and William Robertson. Black-Box Attacks Against Neural Binary Function Detection. In *Proceedings of the International Symposium on Research in Attacks, Intrusions and Defenses*, 2023.

William Blair, William Robertson, and Manuel Egele. ThreadLock: Native Principal Isolation Through Memory Protection Keys. In *Proceedings of the ACM Asia Conference on Computer and Communications Security*, 2023.

William Blair, William Robertson, and Manuel Egele. MPKAlloc: Efficient Heap Meta-data Integrity Through Hardware Memory Protection Keys. In *Proceedings of the International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*, 2022.

William Blair, Andrea Mambretti, Sajjad Arshad, Michael Weissbacher, William Robertson, Engin Kirda, and Manuel Egele. HotFuzz: Discovering Temporal and Spatial Denial-of-Service Vulnerabilities Through Guided Micro-Fuzzing. *ACM Transactions on Privacy and Security* 25, 4 (November 2022).

Andrea Mambretti, Alexandra Sandulescu, Alessandro Sorniotti, William Robertson, Engin Kirda, and Anil Kurmus. Bypassing Memory Safety Mechanisms through Speculative Control Flow Hijacks. In *Proceedings of the IEEE European Symposium on Security and Privacy*, 2021.

Andrew Fasano, Tiemoko Ballo, Marius Muench, Tim Leek, Alexander Bulekov, Brendan Dolan-Gavitt, Manuel Egele, Aurélien Francillon, Long Lu, Nick Gregory, Davide Balzarotti, and William Robertson. SoK: Enabling Security Analyses of Embedded Systems via Rehosting. In *Proceedings of the ACM Asia Conference on Computer and Communications Security*, 2021.

Joshua Bundt, Andrew Fasano, Brendan Dolan-Gavitt, William Robertson, and Tim Leek. Evaluating Synthetic Bugs. In *Proceedings of the ACM Asia Conference on Computer and Communications Security*, 2021.

Seyed Ali Mirheidari, Sajjad Arshad, Kaan Onarlioglu, Bruno Crispo, Engin Kirda, and William Robertson. Cached and Confused: Web Cache Deception in the Wild. In *Proceedings of the USENIX Security Symposium*, 2020.

William Blair, Andrea Mambretti, Sajjad Arshad, Michael Weissbacher, William Robertson, Engin Kirda, and Manuel Egele. HotFuzz: Discovering Algorithmic Denial-of-Service Vulnerabilities Through Guided Micro-Fuzzing. In *Proceedings of the ISOC Network and Distributed System Security Symposium*, 2020.

Amin Kharraz, Brandon L Daley, Graham Z Baker, William Robertson, and Engin Kirda. USBESAFE: An End-Point Solution to Protect Against USB-Based Attacks. In *Proceedings of the International Symposium on Research in Attacks, Intrusions, and Defenses*, 2019.

Kaan Onarlioglu, William Robertson, and Engin Kirda. Eraser: Your Data Won't Be Back. In *Proceedings of the IEEE European Symposium on Security and Privacy*, 2018.

A. Kharraz, W. Robertson, and E. Kirda. Surveylance: Automatically Detecting Online Survey Scams. In *Proceedings of the IEEE Symposium on Security and Privacy*, 2018.

Michael Weissbacher, Enrico Mariconti, Guillermo Suarez-Tangil, Gianluca Stringhini, William Robertson, and Engin Kirda. Ex-Ray: Detection of History-Leaking Browser Extensions. In *Proceedings of the Annual Computer Security Applications Conference*, 2017.

Tobias Lauinger, Abdelberi Chaabane, Ahmet Salih Buyukkayhan, Kaan Onarlioglu, and William Robertson. Game of Registrars: An Empirical Analysis of Post-Expiration Domain Name Takeovers. In *Proceedings of the USENIX Security Symposium*, 2017.

Tobias Lauinger, Abdelberi Chaabane, Sajjad Arshad, William Robertson, Christo Wilson, and Engin 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 System Security Symposium*, 2017.

William Koch, Abdelberi Chaabane, Manuel Egele, William Robertson, and Engin Kirda. Semi-Automated Discovery of Server-based Information Oversharing Vulnerabilities in Android Applications. In *Proceedings of the ACM SIGSOFT International Symposium on Software Testing and Analysis*, 2017.

Ahmet Salih Buyukkayhan, Alina Oprea, Zhou Li, and William 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*, 2017.

Andrea Mambretti, Kaan Onarlioglu, Collin Mulliner, William Robertson, Engin Kirda, Federico Maggi, and Stefano Zanero. Trellis: Privilege Separation for Multi-user Applications Made Easy. In *Proceedings of the International Symposium on Research in Attacks, Intrusions, and Defenses (Lecture Notes in Computer Science)*, 2016.

Amin Kharraz, Sajjad Arshad, Collin Mulliner, William Robertson, and Engin Kirda. UNVEIL: A Large-Scale, Automated Approach to Detecting Ransomware. In *Proceedings of the USENIX Security Symposium*, 2016.

Yanick Fratantonio, Antonio Bianchi, William Robertson, Engin Kirda, Christopher Kruegel, and Giovanni Vigna. TriggerScope: Towards Detecting Logic Bombs in Android Applications. In *Proceedings of the IEEE Symposium on Security and Privacy*, 2016.

Brendan Dolan-Gavitt, Patrick Hulin, Engin Kirda, Timothy Leek, Andrea Mambretti, William Robertson, Frederick Ulrich, and Ryan Whelan. LAVA: Large-Scale Automated Vulnerability Addition. In *Proceedings of the IEEE Symposium on Security and Privacy*, 2016.

Michael Weissbacher, William Robertson, Engin Kirda, Christopher Kruegel, and Giovanni Vigna. ZigZag: Automatically Hardening Web Applications Against Client-side Validation Vulnerabilities. In *Proceedings of the USENIX Security Symposium*, 2015.

Michael Weissbacher, Tobias Lauinger, and William Robertson. Why Is CSP Failing? Trends and Challenges in CSP Adoption. In *Research in Attacks, Intrusions and Defenses (Lecture Notes in Computer Science)*, 2014.

Ting-Fang Yen, Alina Oprea, Kaan Onarlioglu, Todd Leetham, William Robertson, Ari Juels, and Engin Kirda. Beehive: Large-Scale Log Analysis for Detecting Suspicious Activity in Enterprise Networks. In *Proceedings of the Annual Computer Security Applications Conference*, 2013.

Kaan Onarlioglu, Collin Mulliner, William Robertson, and Engin Kirda. PrivExec: Private Execution as an Operating System Service. In *Proceedings of the IEEE Symposium on Security and Privacy*, 2013.

Collin Mulliner, Jon Oberheide, William Robertson, and Engin Kirda. PatchDroid: Scalable Third-Party Security Patches for Android Devices. In *Proceedings of the Annual Computer Security Applications Conference*, 2013.

Leyla Bilge, Davide Balzarotti, William Robertson, Engin Kirda, and Christopher Kruegel. Disclosure: Detecting Botnet Command and Control Servers through Large-Scale NetFlow Analysis. In *Proceedings of the Annual Computer Security Applications Conference*, 2012.

William Robertson and Giovanni Vigna. Static Enforcement of Web Application Integrity Through Strong Typing. In *Proceedings of the USENIX Security Symposium*, 2009.

William Robertson, Giovanni Vigna, Christopher Kruegel, and Richard A Kemmerer. Using Generalization and Characterization Techniques in the Anomaly-based Detection of Web Attacks. In *Proceedings of the ISOC Network and Distributed System Security Symposium*, 2006.

Christopher Kruegel, Engin Kirda, Darren Mutz, William Robertson, and Giovanni Vigna. Polymorphic Worm Detection Using Structural Information of Executables. In *Proceedings of the International Symposium on Recent Advances in Intrusion Detection*, 2006.

Christopher Kruegel, Giovanni Vigna, and William Robertson. A Multi-Model Approach to the Detection of Web-Based Attacks. *Computer Networks* 48, 5 (August 2005).

Christopher Kruegel, Engin Kirda, Darren Mutz, William Robertson, and Giovanni Vigna. Automating Mimicry Attacks Using Static Binary Analysis. In *Proceedings of the USENIX Security Symposium*, 2005.

Christopher Kruegel, William Robertson, and Giovanni Vigna. Detecting Kernel-Level Rootkits Through Binary Analysis. In *Proceedings of the Annual Computer Security Applications Conference*, 2004.

Christopher Kruegel, William Robertson, Fredrik Valeur, and Giovanni Vigna. Static Disassembly of Obfuscated Binaries. In *Proceedings of the USENIX Security Symposium*, 2004.

Selected Invited Talks

It Was the Best of Times, It Was the “Blurst” of Times: On the Dangers of AI and Security	DARPA DSO Colloquium	November 2022
How I Learned to Stop Worrying and Love the Bug	Georgia Tech Cybersecurity Lecture Series	October 2021
Security Through Deception	Schloss Dagstuhl Cybersafety Seminar	September 2019
Capturing Cybersecurity Skills	Army Cyber Day	April 2019
A Maze of Twisty Little Passages, All Alike: A Large-Scale Analysis of Web Proxy Path Confusion	Hakone Cybersecurity Workshop	March 2019
TriggerScope: Detecting Malicious Functionality without Application Specifications	Rensselaer Polytechnic Institute	May 2017
TriggerScope: Detecting Malicious Functionality without Application Specifications	MITLL CORE Series	May 2016
CrossFire: An Analysis of Firefox Extension-Reuse Vulnerabilities	BlackHat Asia	March 2016
How to Get Away with Malware	Stony Brook University	March 2016
How to Get Away with Malware	Chalmers University	February 2016
Future Directions in Defending Industrial Control Systems	ONR ICS Security Workshop	January 2015
Congressional Briefing on Cybersecurity	Capitol Hill, Washington DC	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
Systems Security	NYU Polytechnic	May 2013
Large-Scale, Wide-Area Botnet Detection	Symantec Research Labs	January 2012
Recent Directions in Web Application Security	UMass Lowell	November 2011
Web Application Anomany Detection in a Web 2.0 World	Schloss Dagstuhl	April 2009

Miscellaneous

Citizenship	United States
Citations	9408
h-index	43