William Blair

SpaceX
Washington, D.C.
U.S.A.

url: https://wdblair.io
associations: ACM, IEEE
google scholar

Current Position

Senior Security Software Engineer, Space Exploration Technologies Corporation

Research Interests

I am broadly interested in language-based security topics. I previously worked as the security point of contact (SPOC) for the Graal platform at Oracle Labs where I worked on control-flow integrity (CFI), language and runtime fuzz testing, intra-process isolation, and software supply chain security. During my PhD, I explored how binary analysis tools can inform runtime monitors for microservices while interning in the Cyber Security Intelligence (CSI) team at IBM Research where I participated in the DARPA Cyber-Hunting at Scale (CHASE) program. I used memory protection keys (MPKs) available in recent Intel CPUs to improve applications' memory safety. This was done as a part of the NSF Secure and Trustworthy Cyberspace (SaTC) Taming Memory Corruption with Security Monitors program.
Earlier in my PhD, I worked on *micro-fuzzing*, a novel fuzz testing technique to detect algorithmic complexity (AC) vulnerabilities in production Java programs and libraries during the DARPA Space and Time Analysis for Cybersecurity (STAC) program. The micro-fuzzing prototype, HotFuzz, has detected previously unknown vulnerabilities in the Java Runtime Environment (JRE) which were confirmed by Oracle and IBM. HotFuzz has also found bugs in widely used Java libraries, including `org.json`.

Education

2014-2023 PhD in Computer Science, Boston University
Thesis: *Detecting and Mitigating Software Security Vulnerabilities Through Secure Environment Programming*
Advisors: Manuel Egele, Hongwei Xi

2012-2014 MS in Computer Science, Boston University
Project: *Dependent Types for Real Time Constraints*
Advisor: Hongwei Xi

2008-2012 BA in Computer Science, Boston University

Publications

2024 Matteo Oldani, William Blair, Lukas Stadler, Zbyněk Šlachrt, Matthias Neugschwandtner BinSweep: Reliably Restricting Untrusted Instruction Streams with Static Binary Analysis and Control-Flow Integrity. In Proceedings of the ACM Cloud Computing Security Workshop (CCSW), Salt Lake City, UT, US, October 2024.

2024 William Blair, Frederico Araujo, Teryl Taylor, Jiyong Jang. Automated Synthesis of Effect Graph Policies for Microservice-Aware Stateful System Call Specialization. In Proceedings of the IEEE Symposium on Security and Privacy (Oakland), San Francisco, CA, US, May 2024.

2023 Mark Lemay, Qiancheng Fu, William Blair, Cheng Zhang, Hongwei Xi. A Dependently Typed Language with Dynamic Equality. In Proceedings of the ACM SIGPLAN International Workshop on Type-Driven Development (TyDE), Seattle, WA, US, September 2023.

2023 William Blair, William Robertson, Manuel Egele. ThreadLock: Native Principal Isolation Through Memory Protection Keys. In Proceedings of the ACM ASIA Conference on Computer and Communications Security (ASIACCS), Melbourne, VIC, Australia, July 2023.

2022 William Blair, William Robertson, Manuel Egele. MPKAlloc: Efficient Heap Meta-Data Integrity Through Hardware Memory Protection Keys. In Proceedings of the Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA) Cagliari, Sardinia Italy, June 2022.

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

2021 Leila Delshadtehrani, Sadullah Canakci, William Blair, Manuel Egele, Ajay Joshi. FlexFilt: Towards Flexible Instruction Filtering for Security. In Proceedings of the Annual Computer Security Applications Conference (ACSAC) December 2021.

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

2017 William Blair, Hongwei Xi. Dependent Types for Multi-Rate Data Flows in Synchronous Programming. In Post-Proceedings of the ACM ML/OCAML Workshop September 2015.

Patents

2024 Matthias Neugschwandtner, William Blair. Method for control flow isolation with protection keys and indirect branch tracking. US Patent 11,977,889

2023 Frederico Araujo, William Blair, Sanjeev Das, Jiyong Jang. Guided Micro-Fuzzing through Hybrid Program Analysis. US Patent 11,822,673

2023 Frederico Araujo, William Blair, Teryl Paul Taylor. Stateful Microservice-Aware Intrusion Detection. US Patent 11,720,667

2023 Frederico Araujo, Teryl Paul Taylor, Jiyong Jang, William Blair. Intrusion Detection in Micro-Services through Container Telemetry and Behavior Modeling. US Patent 11,748,473

2023 Frederico Araujo, William Blair, Teryl Paul Taylor. Automated Synthesis of Reference Policies for Runtime Microservice Protection. US Patent Application 17/390,881

Talks

2021 Symbolic Modeling of Micro Services for Intrusion Detection
IEEE Symposium on Security and Privacy Poster Session 2021

2021 Microservice-Aware Reference Monitoring through Hybrid Program Analysis
FloCon 2021 at CMU Software Engineering Institute (SEI)

2019 HotFuzz: Finding Space and Time Vulnerabilities in Java Programs
DARPA Space and Time Analysis for Cybersecurity P.I. Meeting

2016 Continuum: Finding Space and Time Vulnerabilities in Java Programs
DARPA Space and Time Analysis for Cybersecurity P.I. Meeting

2016 Side Channels and Worst Case Behavior in Java
Northeastern-WPI Seminar on Security

2015 Using a Portfolio of SMT Solvers in Software Development
NEPLS Fall at Tufts University

2015 Dependent Types for Real Time Constraints
ACM Sigplan ML Workshop at ICFP 2015

2015 Integrating SMT into Software Development
NEPLS Spring at Wesleyan University

2014 Debugging with types in ATS
Boston Haskell Meetup

Service

2025 Program Committee member for the ACM ASIA Conference on Computer and Communications Security

2024 Secretary for the IEEE Washington D.C. Section

2023 Session Chair for the ACM ASIA Conference on Computer and Communications Security

2022 Sub-Reviewer for the IEEE Symposium on Security and Privacy, IEEE European Symposium on Security and Privacy

2021 Trojan Horse Award reviewer for the IEEE Symposium on Security and Privacy

2021 Shadow Program Committee member for the IEEE Symposium on Security and Privacy

2021 Sub-Reviewer for NDSS, USENIX Security

2020 Sub-Reviewer for ACM CODASPY, DSN, USENIX Security

2019 Sub-Reviewer for ACM CODASPY

2018 Artifact Evaluation Committee member for ACSAC
2018 Sub-Reviewer for ACSAC, RAID, DIMVA, ACM CODASPY
2017 Artifact Evaluation Committee member for ACSAC
2017 Sub-Reviewer for ACM CODASPY

Teaching

Spring 2021 *TF* for CS210 Computer Systems
Lectured on fundamentals of UNIX and C programming and helped students with their programming assignments. Over the course of the semester students implemented their own calculator that parsed and evaluated mathematical expressions given in infix notation. Their calculators used reverse polish notation (RPN) as an intermediate representation for simple arithmetic equations.

Fall 2020 *TF* for CS630 Graduate Design and Analysis of Algorithms
Fall 2019 Lectured on topics including Linear Algebra, LUP Decomposition, Complexity, Approximation Algorithms, Randomized Algorithms, and Linear Programming. Managed a small team of graders.

Spring 2015 *TF* for CS111 Introduction to Computer Science
Fall 2014 Assisted students through a breadth first introduction to Computer Science that covers programming in Functional, Imperative, and Object Oriented paradigms. Other topics such as Computer Organization, Assembly Programming, and Computational Complexity were briefly introduced as well. The class was adapted from the "CS For All" class developed at Harvey Mudd University. My role included leading discussion sections, grading, and holding office hours.

Spring 2014 *TF* for CS211 Object Oriented Programming
Assisted students with learning Objective C and writing applications for iOS devices. Students first built familiarity with the iOS environment by gradually constructing a tweeting App in iOS, and then developed their own original apps.

Awards

2021 IBM Invention Plateau Award
2020 IBM First Patent Application Award
2020 3rd Place speaker at 7th Annual BU CISE Graduate Student Workshop (CGSW 7.0)
2019 2nd Place speaker at 6th Annual BU CISE Graduate Student Workshop (CGSW 6.0)
2018 Student Travel Award to the IEEE Symposium on Security and Privacy
2016 Sixth Summer School on Formal Techniques at Menlo College
2015 Verification Mentoring Workshop at the International Conference on Computer Aided Verification (CAV)

Professional Experience

2024-present *Senior Security Software Engineer* at Spacex Exploration Technologies Corporation
Working on topics related to securing satellite constellations.

2023-2024 *Senior Member of Technical Staff* at Oracle Labs
Investigated language-based security topics within the Graal Platform, including software supply chain security, control-flow integrity (CFI), fuzz testing, binary analysis, and intra-process isolation.

2019-2021 *Research Intern* at IBM Research, Thomas J. Watson Research Center
Investigated intrusion detection in microservices with the Cyber Security Intelligence (CSI) team. Developed μPolicyCraft, a framework for modeling microservice system call profiles represented as *effect graphs*. Effect graphs are stateful summaries of system call sequences and resources a microservice may interact with during its execution. Policy monitors can then detect policy violations (i.e., intrusions) by looking for deviations from a microservice's effect graph in container telemetry.

2015 *Software Engineer Intern* at ViaSat
Assisted in developing a business process engine (BPE) within Amazon Web Services (AWS) that provided a fault tolerant programming framework for executing and managing workflows across distributed systems.

2013 *Software Engineer Intern* at ViaSat
Investigated how mobile applications received multi-media from content providers by reverse engineering native ARM libraries in Android applications, and using a man-in-the-middle server to augment Javascript applications.

2009-2012 *Software Engineer* at 829 Studios LLC
Designed, implemented, and deployed OfferedLocal, a web application that allows businesses to run location based advertising campaigns across social networks like Facebook and Twitter. The start-up participated in Mass Challenge and was featured in the Demo Fall 2011 Conference.
Developed and maintained the back office system for the Licensing Industry Merchandisers Association (LIMA), along with an online directory of member companies.

2009-2010 *Technician* at BU Electronics Design Facility
Developed firmware for a medical prototype as part of the FLuorescence-Assisted Resection and Exploration (FLARE) project at Beth Israel Deaconess Medical Center. The system allowed an external device to control the power output of lasers and regulated their temperature using Peltier coolers. The firmware featured serial communication, analog to digital controllers (ADC) to measure laser temperature, and proportional integral and derivative (PID) controllers to control the Peltier coolers' temperature via pulse width modulation. Assisted in the design, layout, and testing of circuit boards for Physics experiments, including the Compact Muon Solenoid (CMS) experiment at CERN.