MICHAEL SANDBORN, PH.D.

+1 (813) 240-7013

EDUCATION

Vanderbilt University August 2024
Ph.D. Computer Science, Russel G. Hamilton Scholar Cumulative GPA: 4.0/4.0
Dissertation: *Cross-Abstraction Artifacts to Detect Adverse Manipulation*
Advisors: Jules White, Kevin Leach

Research focus: **Cyber-physical Systems, Computer Security**
Keywords: cybersecurity, artificial intelligence, large language models, systems programming, software security

Vanderbilt University August 2016–December 2019
B.S. Computer Science, B.S. Applied Mathematics Cumulative GPA: 3.5/4.0

SKILLS

Languages	Python, C/C++, SQL
Binary Analysis	Ghidra, angr, Radare2, OFRAK, Cuckoo Sandbox
Infrastructure	Airflow, Beam, Docker, gRPC, K8s, LiveKit, LLVM, Pub/Sub, PyTorch

EXPERIENCE

Arta Finance April 2024–Present
Research Engineer—AI Infrastructure *Remote / Mountain View, CA*

· Co-developed real-time streaming text and audio agent with function calling for personalized wealth planning
· Implemented streaming data pipeline to process millions of daily raw and adjusted equity prices for trading
· Built automated LLM agent evaluation framework to assess synthetic and real user sessions to ensure expected behavior

Athena AI Consulting February 2023–April 2024
Co-Founder & CEO *Nashville, TN*

· Bootstrapped AI consulting firm to 30K MRR building bespoke integrations for e-commerce, defense, and SaaS clients
· Led research to achieve 99% accuracy in structured PDF extraction for US IRS tax forms in a stealth SaaS prototype

DARPA Assured Micro-Patching October 2022–May 2024
Graduate Research Assistant—PI: Dr. Baris Kasikci *Nashville, TN*

· Co-developed Transformer model to predict C source code from binary decompilation to facilitate binary micro-patching
· Built lightweight classifier achieving 98% accuracy in predicting compiler optimization flags from ARM binaries
· Contributed to 1M parameter vulnerability detection model using ASTs and embeddings for efficient code security triaging

DARPA Symbiotic Cyber-Physical Systems October 2020–February 2023
Graduate Research Assistant—PI: Peter Volgyesi *Nashville, TN*

· Automated inertial property extraction from CAD models, achieving 100x speedup in UAV design space exploration
· Developed graph neural network drag surrogate models to predict aerodynamic profiles enabling faster design iteration
· Built Python library for UAV trajectory analysis and controller visualization, accelerating design validation cycles

Etsy, Inc. May 2019–August 2019
Software Engineering Intern—Seller Ads & Insights *New York, NY*

· Developed features for an ads dashboard for web (React) and mobile (React Native) serving over 2 million sellers on Etsy.com
· Identified and corrected an existing bug in production code for parsing non-US currency input for seller advertising budgets

Vanderbilt Men's Varsity Baseball August 2016–February 2019
Left-handed Pitcher *Nashville, TN*

· 2019 NCAA National Champion; dedicated 30+ hrs/week year round to baseball training and team meetings
· SEC Athlete Honor Roll recipient, 2-time Dean's list recipient, Omaha Challenge conditioning week winner for pitchers

SELECTED PUBLICATIONS

Yifan Zhang, Michael Sandborn, Stefan Larson, Yu Huang, Kevin Leach, *Structure-Aware Adaptation of LLMs for Code Vulnerability Detection*, Hot Topics in the Science of Security (HotSoS) 2025, accepted.

Michael Sandborn, Zach Stoebner, Wes Weimer, Stephanie Forrest, Ryan Dougherty, Jules White, Kevin Leach, *Reducing Malware Analysis Overhead with Coverings*, Transactions on Dependable and Secure Computing (TDSC) 2024, to appear.

Michael Sandborn, Carlos Olea, Anwar Said, Mudassir Shabir, Peter Volgyesi, Xenofon Koutsoukos, Jules White, *Towards AI-Augmented Design Space Exploration Pipelines for UAVs*, Book series: Intelligent Computing. Artificial Intelligence (Machine Learning, Convolutional Networks and Large Language Models). Edited by Leonidas Deligiannidis, George Dimitoglou, Hamid Arabnia and Ahmad Tafti. Publisher: De Grouyter.

Henry Gilbert, Michael Sandborn, Douglas C. Schmidt, Jesse Spencer-Smith, Jules White, *Semantic Compression with Large Language Models*, 2023, Preprint.

Harsh Vardhan, Umesh Timalsina, Michael Sandborn, Peter Volgyesi, Janos Sztipanovits, *Anvil: A SciML tool for CFD-based design evaluation with AI-powered shape optimization algorithms*, 6th Workshop on Design Automation for CPS and IoT (DESTION) 2024.

Jules White, Quchen Fu, Sam Hays, Michael Sandborn, Carlos Olea, Henry Gilbert, Ashraf Elnashar, Jesse Spencer-Smith, Douglas C Schmidt *A prompt pattern catalog to enhance prompt engineering with chatgpt*, 2022, Preprint.

Michael Sandborn, Carlos Olea, Anwar Said, Mudassir Shabbir, Peter Volgyesi, Xenofon Koutsoukos, Jules White, *What a drag! Streamlining the UAV design process with design grammars and drag surrogates*, International Conference on Computational Science and Computational Intelligence (CSCI) 2022 (**24% Acceptance Rate**), in proceedings.

Michael Sandborn, Carlos Olea, Jules White, Chris Williams, Pablo Tarazaga, Logan Sturm, Mohammad Albakri, Charles Tenney. *Towards Secure Cyber-physical Information Association for Parts*, Journal of Manufacturing Systems, Volume 59, April 2021 **(8.63 Impact Factor, 18% Acceptance Rate)**.

SELECTED PRESENTATIONS & SERVICE

Montgomery County AI Council August 2025 - Present
Advisor *Montgomery County, PA*

· Elected to the Advisory Council on AI for Public Good in Montgomery County, PA. Contribute to county board discussions and prototype AI tools to improve community technology posture.

HotSoS 2025 (NSA-Sponsored Computer Security Conference) Spring 2025
Reviewer *Remote*

· Reviewed submitted manuscripts of computer security contributions for technical novelty and research quality.

DARPA Assured Micro-Patching PI Meeting May 2024
Research Assistant *Greenbelt, MD*

· Presented to DARPA AMP stakeholders and PIs at the NASA Goddard Space Flight Center about Vanderbilt's efforts in improving the assurance and quality of binary micropatches using AI techniques such as compiler provenance prediction, canonical source code recovery, and ARM cache side-channel detection.

DESTION 2024 May 2024
Author Presentation *Remote*

· Presented to attendees of the DESTION 2024 workshop in Hong Kong about Anvil, a tool to accelerate design iteration of multi-terrain vehicles by combining Computational Fluid Dynamics (CFD) analysis artifacts with Bayesian optimization algorithms and efficient sampling techniques.