

Burak Kadron

Software Engineer, Security Tooling | PhD in Computer Science

📍 Santa Barbara, CA ✉ kadron.burak@gmail.com ☎ (805) 284-6115 🌐 kadron.github.io 🌐 kadron
🔗 kadron 📄 Google Scholar

Summary

Software engineer and security researcher with a PhD in program analysis and 4 years building fuzzing and constraint-solving tools for smart-contract security. Experienced in language design (parsers, interpreters, DSLs), input generation, and side-channel analysis, with publications at NDSS, ESEC/FSE, ISSTA, and ASE.

Experience

Veridise, Research Scientist

Remote

Nov 2022 – present

- Lead engineer on OrCa, Veridise's fuzzer for Solidity smart contracts (Python), used across the company's security audits
- Rewrote the LTL-based [V] specification language end to end: updated ANTLR grammar, a generator that converts parse trees to an intermediate representation, and the interpreter
- Designed and built from scratch a hint language that lets users specify how functions are fuzzed; user constraints are compiled to SMT-LIB and solved with Z3 to generate function inputs
- Added on-chain fuzzing support, enabling OrCa to test deployed contracts against live chain state
- Maintained OrCa's Rust EVM component, keeping it in sync with upstream dependencies including Foundry's EVM
- Refactored core fuzzing components, improving performance and coverage
- Performed smart-contract and infrastructure security audits for 3 client protocols: ThetaNuts, Manta Network, and Stellar (Soroban core)

University of California, Santa Barbara, Graduate Student Researcher

Santa Barbara, CA

Jan 2017 – Sept 2022

- Developed techniques to detect, quantify, and mitigate side-channel information leakage in encrypted network traffic
- Built [TSA](#), an open-source tool for network side-channel detection and quantification
- Published at NDSS, ISSTA, and ESEC/FSE; represented UCSB Verification Lab in DARPA's STAC (Space/Time Analysis for Cybersecurity) program
- Mentored one Master's and two undergraduate students on research projects, including CorbFuzz, a fuzzer for checking browser security policies (ASE 2021)

NASA Ames Research Center (KBR Inc.), Research Intern

Remote

June 2020 – Sept 2020

- Analyzed robustness of Boeing's runway-image neural network for autonomous center-line tracking
- Built a concolic analysis method that uses the Marabou verifier to check robustness to input perturbations and generate counterexample images
- Published findings as a case study (VSTTE 2021)

Carnegie Mellon University, CyLab, Research Intern

Moffett Field, CA

June 2018 – Sept 2018

- Developed input generation techniques for side-channel analysis; represented CMU CyLab in DARPA STAC
- Worked on adversarial input generation for neural networks using symbolic execution (ISSRE 2019)

University of California, Santa Barbara, Teaching Assistant
• Data Structures & Algorithms I & II, Formal Languages & Automata

Santa Barbara, CA
Sept 2016 – June 2018

Airties Wireless Networks, Systems & Research Engineer (Part-time)
• Implemented mesh-networking code in C supporting client handover between Wi-Fi routers

Istanbul, Türkiye
June 2013 – Sept 2015

Education

PhD **University of California, Santa Barbara**, Computer Science
• Dissertation: Detection, Quantification and Mitigation of Network Side Channels
• Advisor: Tevfik Bultan
• Committee: Tevfik Bultan, Giovanni Vigna, Yu-Xiang Wang

Santa Barbara, CA
Sept 2016 – Sept 2022

BS **Boğaziçi University**, Computer Engineering

Istanbul, Türkiye
Sept 2010 – June 2014

Skills

Languages: Python, Rust, Solidity, Java, C, Bash

Interests: Fuzzing, formal methods, side-channel analysis, SMT-based constraint solving, concolic/symbolic execution, smart-contract auditing

Tools: Z3, CVC5, ANTLR, Foundry, EVM, Docker, Git

Selected Publications

Fuzzing, Symbolic Execution, and Expert Guidance for Better Testing

Jan 2023

Burak Kadron, Yannic Noller, Rohan Padhye, Tevfik Bultan, Corina S. Păsăreanu, Koushik Sen
(IEEE Software)

TSA: A Tool to Detect and Quantify Network Side-Channels

Nov 2022

Burak Kadron, Tevfik Bultan
(ESEC/FSE 2022)

CorbFuzz: Checking Browser Security Policies with Fuzzing

Nov 2021

Chaofan Shou, **Burak Kadron**, Qi Su, Tevfik Bultan
(ASE 2021)

Feedback-Driven Side-Channel Analysis for Networked Applications

July 2020

Burak Kadron, Nicolás Rosner, Tevfik Bultan
(ISSTA 2020)

Profit: Detecting and Quantifying Side Channels in Networked Applications

Feb 2019

Nicolás Rosner, **Burak Kadron**, Lucas Bang, Tevfik Bultan
(NDSS 2019)