# BENJAMIN DEMICK

ben.demick@gmail.com | (919) 999-6191 | Raleigh, NC

## Professional Summary

Security research engineer with 20+ years specializing in hard target vulnerability research: embedded firmware, RTOS, and bare-metal systems across heterogeneous architectures and platforms, where traditional techniques often fall short. Validates vulnerabilities through working proof-of-concept exploits and coordinates non-public disclosure. Builds automated program analysis and symbolic execution tooling (angr, Z3) for reproducible, auditable research. Applies AI-assisted workflows, including emulator bring-up and AI-generated fuzzing harnesses to extend coverage on hard targets, paired with manual verification. US patent holder for an automated vulnerability analysis framework, co-founder of a security research lab, and comfortable defining and documenting methodology for independent review.

## Relevant Skills

**Security Research & Exploitation:** Vulnerability discovery and validation, exploit development (memory corruption, ROP), proof-of-concept development, responsible disclosure, threat modeling, secure code review

**Program & Binary Analysis:** Static and dynamic analysis, symbolic execution (angr, Z3), automated triage and reachability tooling, emulation (qemu, Unicorn, Simics), Kaitai Struct

**AI-Assisted Research:** LLM-assisted vulnerability research and analysis workflows; AI-generated fuzzing harness construction for embedded/hard target systems; Claude Code, Codex

**Programming:** C, C++, Python, Assembly (ARM, x86/x86_64, RISC-V, PowerPC, MIPS, 68k), C#, JavaScript

**Tooling:** IDA Pro, Ghidra, Binary Ninja, radare2, gdb, WinDbg, GNU toolchains, Git, pytest

## Experience

**Reverse Engineer (Team Lead)** | *Kudu Dynamics* Feb 2023 – Present

- Leads a team of eight researchers performing hard target vulnerability research and validation across embedded firmware spanning ARM, x86, RISC-V, MIPS, and PowerPC architectures (bare metal, RTOS, Linux).
- Applies AI-assisted analysis workflows, including AI-generated fuzzing harness construction, to extend research coverage on hard targets where traditional fuzzing has limited reach; in one case, work that previously took a team of four researchers a year was completed by one researcher in a week.
- Designed and led development of an automated static analysis triage engine for monolithic firmware binaries, confirming vulnerability reachability and improving reviewer context.
- Builds program analysis tooling with Ghidra, Binary Ninja, IDA Pro, C, C#, JavaScript, Python, and Kaitai Struct for vulnerability discovery and validation.
- Collaborates with platform engineering and product teams to define quality standards for validated findings.

**Principal Security Researcher** | *Finite State, Inc.* Jun 2020 – Dec 2022

- Led firmware analysis automation initiatives, developing scalable binary analysis capabilities for vulnerability identification, validation, and metadata extraction across embedded systems.
- Conducted vulnerability research and exploit proof-of-concept development for RTOS, bare metal, and retrofit systems, confirming reachability before escalation.
- Coordinated with engineering teams to translate validated vulnerability discoveries into actionable remediation guidance.

**Senior Security Researcher** | *Booz Allen Hamilton* Oct 2018 – Jun 2020

- Led offensive security research for the TechX program, directing a team of three investigating vulnerabilities in microkernel architectures and novel processor designs.
- Developed automated static analysis tooling to improve vulnerability discovery and validation in complex software systems.
- Researched embedded system emulation techniques for vulnerability testing and exploit development.
- Mentored junior researchers on reverse engineering, vulnerability analysis, and responsible disclosure; led workshops at Defcon 919 and Raleigh ISSA.

**Senior Security Researcher** | *Booz Allen Hamilton* Sep 2014 – Oct 2018

- Founding member of Dark Labs; led vulnerability discovery teams performing responsible disclosure to vendors across consumer electronics, IoT, and industrial control systems.
- Led a four-person team building an automated vulnerability analysis framework, resulting in US Patent 10,133,871.
- Led a three-person team that discovered and demonstrated a practical physical exploit against a critical ICS/SCADA device, driving measurable security improvements.
- Lab instructor for ENEE459B Reverse Engineering and Hardware Security Laboratory, University of Maryland; developed and delivered training at multiple BSides conferences.

**Senior Lead Engineer** | *Booz Allen Hamilton* Jan 2013 – Sep 2014

- Led a reverse engineering project to recover functionality and identify vulnerabilities in undocumented third-party embedded firmware.
- Automated binary analysis and exploit-development workflows using IDAPython, gdb, and Python for scalable, portable tooling.

**Associate** | *Booz Allen Hamilton* Jan 2011 – Dec 2012

- Technical lead for a four-person embedded software reverse engineering project; developed automated binary analysis tools for Windows and VxWorks applications.

**Associate** | *Booz Allen Hamilton* Sep 2009 – Dec 2010

- Led a four-person team building embedded systems hardware virtualization using Wind River Simics, including a custom system emulator synthesized from reverse engineered firmware.

**Electrical Engineer 3** | *Northrop Grumman* Jun 2008 – Sep 2009

- Hardware design and schematic capture (P-CAD); VHDL simulation (ModelSim, Xilinx ISE); test-system engineering in LabVIEW.

**Software Engineer** | *General Dynamics IT* Feb 2005 – Jun 2008

- Developed automated test systems and GUI tooling in LabVIEW, including automated calibration infrastructure with Agilent instrumentation.

**Software Engineering Associate** | *Lockheed Martin IS&S* Oct 2003 – Feb 2005

- Completed training in CMMI methodologies, Lean Six Sigma, and project management.

## Education

**Johns Hopkins University**, M.S., Electrical and Computer Engineering
**Clarkson University**, B.S., Electrical Engineering and Physics

## Patents & Recognition

**US Patent 10,133,871**: Method and system for identifying functional attributes that change the intended operation of a compiled binary extracted from a target system (Co-inventor)

Booz Allen Hamilton Team and Performance Award (3x), Patent Award, New Patent Application Award · General Dynamics Exceptional Performance Award · Clarkson University Presidential Scholar

***Clearance available upon request.***