Benjamin Demick

3420 Edgemont Drive, Raleigh, NC 27612
919.999.6191 ▪ ben.demick@gmail.com ▪ https://epidemix.io/

Skills

Software Tools
Binary Ninja, Ghidra, IDA Pro, Hex-rays decompiler, Kaitai Struct, Capstone, Unicorn, qemu, binwalk, angr, Valgrind, GNU binutils, radare2, YARA, LIEF, pyelftools, OllyDbg, Immunity Debugger, Wireshark, Simics, SQLite, Z3, Qt, Lucidchart, Visio

Programming Languages
C, C++, Assembly (Power PC, x86, RISC-V, ARM, x86_64, MIPS, 68k), Python, bash, LaTeX, Java, IDAPython, Jython, LLVM IR, VHDL, LabVIEW, MATLAB, HTML, SCPI, SQL, C#, Javascript

Operating Systems & Platforms
Linux, VxWorks, Windows, macOS, UNIX, Zephyr, QNX, FreeRTOS

Development Tools
GNU embedded toolchains, gdb, clang, Git, WinDbg, PyCharm, unittest, JIRA, Confluence, Microsoft Visual Studio, Tornado, Cygwin, Subversion, Redmine, Smart Bear Collaborator, ModelSim, P-CAD, Xilinx ISE, LTSpice

Education

Johns Hopkins University, *Baltimore, MD* (2007-2010) Master of Science, Electrical and Computer Engineering

Clarkson University, *Potsdam, NY* (1999-2003) Bachelor of Science, Electrical Engineering and Physics

Patents

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)

Experience

Kudu Dynamics, *Chantilly, VA* (February 2023 - present)
Reverse Engineer
- Performs static and dynamic analysis of software across a broad variety of systems, to include embedded, Linux, and Windows (.NET and native C++) applications
- Develops automated analysis tools using Ghidra, Binary Ninja, C#, Javascript, Python, Kaitai Struct, and WinDbg for software introspection and measurement

Finite State, Inc., *Raleigh, NC* (June 2020 - December 2022)
Principal Security Researcher
- Led firmware analysis automation and developed binary analysis capabilities for metadata extraction, driving insight into firmware composition and risk
- Performed novel research and proof of concept development in embedded firmware static and dynamic analysis based on academic and industry research for retrofit, RTOS, and bare metal systems

Booz Allen Hamilton, *Washington, DC* (September 2009 - June 2020)
Senior Security Researcher, Cyber Account (October 2018 - June 2020)
- Led advanced security research projects for the TechX program
- Led team researching nascent microkernel OS design and security and emerging processor architectures
- Performed research on embedded system emulation
- Developed research program with local universities
- Guided strategic research initiatives and mentored research projects
- Led Software Reverse Engineering workshops at Defcon 919 Meetup and Raleigh ISSA

Senior Security Researcher, Dark Labs (September 2014 - October 2018)

- As founding member of Dark Labs, led embedded system security research projects to perform vulnerability discovery, proof of concept exploit development, and responsible disclosure to vendors
- Led research team in development of novel approach and framework for analyzing embedded system firmware, resulting in US Patent 10,133,871
- Led 4-person research team in discovery of practical physical attack against a critical ICS/SCADA device for a client, presented results to client which facilitated a demonstrable improvement in security practices
- Authored technical content for multiple commercial RFPs
- Authored blog posts on firmware analysis for Dark Labs website
- Lab instructor for ENEE459B Topics in Computer Engineering: Reverse Engineering and Hardware Security Laboratory at University of Maryland College Park
- Co-taught Binary Reverse Engineering for Beginners workshops at multiple BSides conferences
- Instructor and content developer for Booz Allen Hamilton Software Reverse Engineering courses

Senior Lead Engineer, Cyber Account (January 2013 - September 2014)

- Lead research, software and systems engineer for an embedded software project
- Performed static and dynamic reverse engineering using COTS, FOSS, and client-developed tools to recover functionality of undocumented software and augment with new features
- Performed software vulnerability analysis and exploitation
- Automated static and dynamic binary analysis using IDAPython, gdb and Python scripting
- Performed system research and development on VxWorks and Linux platforms in C and assembly
- Advised client on technical direction, communicated project status and participated in technical exchanges
- Analyzed, derived and documented system-level requirements
- Authored research, technical approach, high level design, system architecture, unit design, test, and interface control documentation
- Guided software design process through the full software development lifecycle, designing modular software
- Career manager for four staff members, developed technical talent on project team
- Instructor and content developer for Booz Allen Hamilton Software Reverse Engineering courses
- Booz Allen Hamilton DIG Cyber Technical Innovator, performed self-directed computer security research
- Contributed technical subject matter expertise to several procurement efforts

Associate, Cyber Account (January 2011 - December 2012)

- Technical Task Order Lead for an embedded software project
- Responsible for guiding the full software development lifecycle, system architecture, and design
- Authored technical approach, high level design and unit design documentation
- Created software development and software configuration management guides
- Performed static and dynamic reverse engineering of undocumented Windows x86 and VxWorks Power PC binaries to facilitate understanding of system behavior
- Windows application development in C with Visual Studio
- VxWorks application development in C with GNU tools and Tornado

Associate, Cyber Account (September 2009 - December 2010)

- Led team developing embedded systems hardware virtualization using Wind River Simics
- Created system emulator to run undocumented embedded system software by reversing required hardware models and boot process from binary and iteratively building emulator to include models
- Performed static and dynamic binary software reverse engineering using IDA Pro and Simics for virtual hardware validation

Northrop Grumman, *Annapolis, MD* (June 2008 - September 2009)

Electrical Engineer 3

- Hardware design and schematic capture using P-CAD 2006
- VHDL development for simulation support using ModelSim and Xilinx ISE
- Test system engineering and support using LabVIEW and COTS equipment to create quick-response test systems

General Dynamics Information Technology, *Chantilly, VA* (February 2005 - June 2008)

Software Engineer

- LabVIEW automated test system development, GUI design and individual test programming
- Created graphics for test system and documentation
- Automated test system construction, calibration and development with Agilent instrumentation using GPIB

Lockheed Martin IS&S, *Reston, VA* (October 2003 - February 2005)
Software Engineering Associate

- New Employee Orientation coordinator
- Completed training in CMMI methodologies, Lean Six Sigma and project management

Clarkson University Physics Department, *Potsdam, NY* (August 2002 - May 2003)
Teaching Assistant

- Undergraduate teaching assistant for freshman physics sequence of mechanics and electromagnetics
- Duties included leading lab and recitation sessions for one 25-student section
- Graded labs, homework and exams, proctored exams and held office hours

Awards and Activities

Booz Allen Hamilton Team and Performance Award (3), Booz Allen Hamilton New Patent Application Award, Booz Allen Hamilton Patent Award, General Dynamics Information Technology Exceptional Performance Award, Clarkson University Presidential Scholar (2 semesters), Dean’s List (5 semesters)