Sean Bradly

SB@NSFW.JP | SBRADLY | RHYTHMX | (512) 677-LULZ
AUSTIN, TEXAS

Security Consultant • Researcher • Developer

About

After 20 years of working in the realm of software engineering and 15 of those focused on entirely on cybersecurity, I have some level of experience in just about every facet of computing, and mastery in quite a few. My greatest skill, and why I currently find myself in consulting, is that I'm able to quickly absorb new subject matter and think outside the box.

I've authored large software projects, audited source code and raw binaries for vulnerabilities, run penetration tests, reverse engineered firmware to verify features, rolled my own fuzzing frameworks, soldered this to that, wrote an operating system, and the list goes on. I have also honed my communication skills while authoring countless reports, whitepapers, presentations, and other media about all of the above, presenting them to coworkers, clients, and audiences at large for deep discussion.

I was naturally drawn into the security space. I have always (ever since I could hold a screwdriver) liked to take things apart to see how they work. I like to imagine all the new and unexpected things that can be built out of all the bits and pieces. Working in computer security has always just that for me; breaking things down into components and getting to the ground truth of what is possible.

Skills:

- **General**: Security, R&D, Reversing, Exploiting, Networking, Hardware, Automation
- **Languages**: C, C++, Ruby, Python, Assembly, Shell, Lisp, Java
- **Architectures**: X86, X86_64, ARM, PIC, OpenRISC, Z80, Hexagon
- **Software**: Linux, Windows, GCC, Clang, GDB, Emacs, IDA, Ghidra, Burp

Personal Interests:

- **Aviation**: I'm currently working towards my private pilot's license
- **Cooking**: Modernist cuisine and science experiments for dinner!
- **Career**: Reading, tinkering, and attending conferences or local meetups to socialize and stay current
- **Other**: Music (guitars, bass, drums, et. al), woodworking, video games

Highlighted Projects

Secure Embedded Operating System

Inverse Limit (for Google) • *2014-2015*

As part of Google ATAP's Project Vault, Inverse Limit's small team of 4 designed and developed a complete computer platform with a security focus. All components are open source; the board schematics, OS, applications, drivers, toolchain, emulator, and even the CPU (based on OpenRISC) have been released to GitHub. Among other things, I was solely responsible for implementing the real-time multitasking operating system for the project.

Launch video (Google I/O 2015): **http://goo.gl/5mZrVR**
Source code: **http://goo.gl/0pbsk7**

X86 Hypervisor and CPU Instruction fuzzer

Inverse Limit (for DARPA) • *2013*

The MAIM project (Micro-architecture Instruction Mining) was one of three Cyber Fast Track proposals that DARPA accepted from Inverse Limit. It consisted of an x86 instruction fuzzer and a cross-platform hypervisor to execute the instructions and compare their behavior on different implementations. The project identified several undocumented differences between Intel, AMD and VIA architectures.

Whitepaper: **http://goo.gl/Kwa3Rf**

Complete TCP/IP Stack for Attack Traffic

BreakingPoint Systems • *2010-2011*

I redesigned BreakingPoint's existing network security test framework from a traffic simulator into a fully featured TCP/IP stack that could test live applications while transparently applying any number of advanced network evasion techniques. At the same time, by integrating concurrency into the new design and strategically replacing components with C extensions, the performance was quadrupled.

Complete work history and references are available upon request. For resume LaTeX source, see https://github.com/rhythmx/resume

Work History

Atredis Partners, LLC

Principal Research Consultant • ***2017-current***

Atredis is an industry leader in security consulting. Focus is placed on bespoke consulting engagements, specifically tailored to the individual client's particular niche. As a Principal at Atredis, I am responsible for leading the technical effort as the main point of contact with clients and for organizing and directing the efforts of other members of the consulting team.

Hardware / Embedded

- UEFI Reverse Engineering
- DSP Reverse Engineering (Hexagon)
- Secure Boot Reviews
- Hypervisor Testing and Source Reviews
- Baseboard Management Controller Reviews
- Device Driver Audits

Mobile

- Android Application Binary/Source Review
- Vendor HLOS Component/Configuration Review
- Trustlet Reverse Engineering
- Feature Development

Miscellaneous

- Technical Writing and Presentation
- Blockchain Application Reviews
- Custom Fuzzer Development
- Web Application Assessments
- Cloud Configuration Reviews
- Network Penetration Tests

Inverse Limit, LLC

Security Engineer and Researcher • ***2013-2017***

Inverse Limit was a research and engineering contracting company that was formed in 2013 ago with my colleagues Patrick Stach and Tim Carstens, supported by notable clients such as Google and DARPA.

Project Vault

- Embedded OS (see projects)
- Developed IO model using FAT filesystem
- Drivers for Custom Hardware
- Android Prototype Application
- Designed entire project layout and build system
- Hardware and Software completely open source

Project MAIM

- Custom x86 hypervisor (see projects)
- Co-Implemented x86/x64 instruction fuzzer
- Implemented main data analysis engine
- Authored final report with all research results

Other

- Design of new research proposals
- Created Kerberos protocol analysis tools
- Maintained libClang static code analysis tools

Leviathan Security Group, Inc.

Security Consultant and Developer • ***2011-2013***

Leviathan was (at the time) a small consultancy focusing on challenging niche projects. I was brought on to help facilitate long-term R&D projects and to assist the consulting group as needed.

Mayor Myer (DARPA Research Program)

- Created polymorphic x64 shellcode encoder
- GNU libc heap corruption detector
- Intel JIT compiler and emulator

Consulting

- Audited Intel ME firmware
- Developed fuzzer for Intel ME applications
- Audits of embedded Java applications
- Android Research

BreakingPoint Systems Inc. (now Keysight)

Security Engineer • ***2007-2011***

BreakingPoint's product is designed to be an ultra-high performance tool for testing network devices. It generates realistic network traffic at 100+ gigabits per second while monitoring the device under test for reporting.

- Complete TCP/IP implementation in Ruby (see projects)
- Implemented framework for network traffic simulation
- Discovered and reported new 3rd-party vulnerabilities
- Performed differential patch analysis on Microsoft updates monthly
- Maintained product coverage of important security vulnerabilities
- Sample blog posts: **http://goo.gl/8yzJFv** - **http://goo.gl/GnWZGX**

Complete work history and references are available upon request. For resume LaTeX source, see https://github.com/rhythmx/resume