Sean Bradly

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

Austin, Texas

Security Expert • Researcher • Software Engineer

About

With 15 years of experience in the software engineering and computer security fields, I have successfully researched, designed, implemented, maintained and delivered many successful projects in a wide variety of roles with a very broad spectrum of subject matter.

Security is a primary focus because it affords an opportunity to constantly learn new and interesting things. Everything needs a level of security, and using that as an entry point, there will always be broad and ever-expanding aspects of technology to explore.

Skills:

- **General**: Security, R&D, Reversing, Exploiting, Networking, Performance, Embedded
- **Languages**: C, C++, Ruby, Python, Assembly, Shell scripting, Lisp, Java, LaTeX
- **Architectures**: X86, X86_64, ARM, PIC, OpenRISC, Z80, ATmega
- **Software**: Linux, Windows, GCC, Clang, GDB, Emacs, IDA, Autotools, CMake

Personal Interests:

- **Music**: Guitars, bass, drums, brass, synths and recently, a thrash metal ukulele
- **Home Improvement**: My first house has been keeping me busy with plenty of projects
- **Entertaining**: Inviting friends over for smoked meats, craft beers, and fine whisky
- **Career**: Attending conferences and local meetups to socialize and stay current

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.

Work History

Inverse Limit, LLC.

Security Engineer and Researcher • ***2013-2017/04***

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

Project Vault

- Embedded OS (see above)
- Developed IO model using FAT filesystem
- Hardware drivers (GPIO, UART, Flash, Crypto acceleration)
- Android Prototype Application (using native SDK)
- Designed entire project layout and build system

Project MAIM

- Custom x86 hypervisor (see above)
- Implemented generators for a number of x86/x64 instruction types
- Implemented main data analysis engine
- Authored final report with all research results

Other

- Design of new research proposals
- Helped design and implement Kerberos protocol analysis tools
- Maintained static code analysis tools written in libClang

Leviathan Security Group

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

Leviathan is 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)

- Designed x64 polymorphic shellcode encoder for Metasploit
- GNU libc heap corruption detector
- Maintained and extended x86 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 Ixia)

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 above)
- 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**

Secured Infrastructure Design Corp. (now defunct)

Security Engineer • ***2006-2007***

SIDC was a small security consulting firm based out of Tokyo, Japan that was developing a web portal allowing customers to setup daily automated security scans.

- Assisted development of automated vulnerability scanner
- Designed distributed TCP/UDP port scanner
- Implemented raw networking C extension for Python
- Relocated to Tokyo for 6 months

GTECH Corp.

Automation Engineer / Systems Administrator • ***2004-2006***

About half (at the time) of the state lotteries in the US were managed by GTECH. As a Systems Administrator at their Austin datacenter, I was directly responsible for the ultra-high availability lottery systems of Texas, California, Idaho, Kansas, Jamaica, and Washington.

- Maintained and operated high volume lottery servers that handle thousands of transactions per minute in an environment where large government fines are imposed for downtime
- Administrated OpenVMS, AIX, Linux, Tru64 Unix, Windows (98, 2000, XP, 2003), MSSQL, and Sybase
- Automated a large part of the Operations department using Perl, Shell (csh and dcl), and BMC Control-M