

Sean Bradly

Computer Security | Software Engineering

Skills

software development
computer security
reverse engineering
research
networking
performance
embedded
electronics
x86
ARM
OpenRISC

Languages

c++
c
assembly
ruby
python
bash
java
lisp
L^AT_EX

Software

linux
windows
gcc
clang
gdb
emacs
ida
autotools
cmake

Contact

Austin, TX
(512) 423-0489
sb@nsfw.jp



About

With 15 years of experience in the software engineering and computer security fields, I have successfully 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 me an opportunity to learn about new things and keep my focus fresh. All software needs a level of security, and using that as an entry point, there will always be a new and interesting corner of computing for me to explore.

Highlights

2014-2015

Designed secure embedded operating system

Inverse Limit (for Google)

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):
Source:

<http://goo.gl/5mZrVR>
<http://goo.gl/0pbsk7>

2013

Implemented a custom x86 hypervisor

Inverse Limit (for DARPA)

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 was able to identify several undocumented differences between Intel, AMD and VIA architectures.

2010-2011

Delivered a complete TCP/IP Stack

BreakingPoint Systems

I took BreakingPoint's existing network security testing framework and completely redesigned it from a traffic simulator into a fully featured TCP/IP stack that could communicate and test live applications. Both versions were implemented in Ruby, but by deeply integrating concurrency into the new design and strategically replacing Ruby components with C extensions, I also managed to quadruple the performance of the already heavily optimized code.

Personal Interests

- **Music:** I play guitars, bass, drums, synths and recently, a thrash metal ukulele
- **Home Improvement:** My recently-purchased first house has been keeping me busy
- **Entertaining:** Inviting friends for some smoked meats, craft beers, and fine whisky
- **Career:** Attending conferences and local meetups to keep current and socialize

Work History

(references available upon request)

Skills

software development
computer security
reverse engineering
research
networking
performance
embedded
electronics
x86
ARM
OpenRISC

Languages

c++
c
assembly
ruby
python
bash
java
lisp
L^AT_EX

Software

linux
windows
gcc
clang
gdb
emacs
ida
autotools
cmake

Contact

Austin, TX
(512) 423-0489
sb@nsfw.jp

2013-now

Inverse Limit, LLC.

Research and Development

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

2011-2013

Leviathan Security Group

Security Consulting and Development

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

2007-2011

BreakingPoint Systems Inc. (now Ixia)

Security Engineer

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 application simulation
- Discovered and reported new 3rd-party vulnerabilities
- Performed differential patch analysis on Microsoft updates monthly
- Maintained product coverage of important security vulnerabilities
- Implemented fuzzers for HTML, HTTP, PDF, OSPF, BGP

Work History (optional page)

(references available upon request)

Skills

software development
computer security
reverse engineering
research
networking
performance
embedded
electronics
x86
ARM
OpenRISC

Languages

c++
c
assembly
ruby
python
bash
java
lisp
L^AT_EX

Software

linux
windows
gcc
clang
gdb
emacs
ida
autotools
cmake

Contact

Austin, TX
(512) 423-0489
sb@nsfw.jp

2006-2007

Secured Infrastructure Design Corp. (now defunct)

Security Engineer

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

2004-2006

GTECH Corp.

Automation Engineer / Systems Administrator

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

2002-2004

Manning Environmental Inc.

Software Engineer

Manning is a small, family-owned business in my hometown that designs and manufactures automatic fluid samplers; essentially robots that periodically pump water from a water treatment system into containers to send to a laboratory.

- Embedded programming for Zilog and Microchip architectures
- Maintained company web site, and several other sites on contract
- Circuit design verification and debugging
- Designed a low-cost microphone-based fluid detection circuit
- Designed production tests for new circuit boards

2000

University of Texas: Applied Research Labs

Java Programmer (paid intern)

I obtained this summer programming internship while still in high school, learned Linux and Java while on-the-job, and completed all of my tasks successfully.

- Updated Java components for a U.S. Department of Defense project
- Assembled and installed new employee PC workstations
- Assisted staff with physical labor of office relocation