

# JESSE DUTTON

---

jessedutton@gmail.com

(508) 697-8489

## Summary

As an expert in more than one computing niche, I am uniquely positioned to tackle new and difficult problems. I have designed operating systems, created systems that effectively detect and track hackers in real time (currently in use by the US government), implemented a distributed database management system that can hold more data than your brain, written linux kernel modules a plenty, reverse engineered hardware protocols and closed source operating systems, designed a city-wide digital telephone system, and done it all with finesse the first time through. Currently located in Boston, MA, and willing to work anywhere in the world.

## Experience

- **Self Employed – Selected Projects—**

*January 2009–Present*

- Implemented a system for developing genetic algorithms for use in robotic systems, and interfaced with a 3D simulation environment to provide a platform where these algorithms could be grown. My system allows many genetic algorithms to be networked together to achieve complex behavior, simplifying the creation of fitness functions, and increasing the complexity possible with a GA system.
- Created a text compression algorithm for extremely compact embedded systems. The decompressor compiles down to 150 bytes of code and achieves a compression rate of 65%.
- Developed a program that adds additional instrument "voices" to a composition, causing the piece to take on a certain mood. This allows video games and other interactive content to change the effect of the music programatically without requiring multiple compositions.
- Assorted consulting related to computer security and application design.

- **NeuralIQ—Santa Monica, CA**

*February 2007–December 2008* NeuralIQ is the leading Intrusion Forensics and Counterintelligence supplier to the US government, and specializes in honey-pot appliances that gather information from hackers. The appliance was divided into three tasks: data collection, analysis, and presentation. I was the architect and primary developer in charge of data collection.

- Created the patent pending data collection method that allowed NeuralIQ's products to see every function call made in every process in both kernel and user space of guest systems. We initially utilized the KVM virtualization software in linux, and later moved to a custom hypervisor.
- As part of this work, created a custom linux kernel module that affected the memory management (e.g. paging) portions of the kernel. In addition, this kernel module implemented a state machine that allowed users to specify memory buffers to be captured as the guest encountered certain function calls in its user processes, or in guest kernel space.
- Reversed engineered parts of Windows XP, 2003, and Vista to find the internal data structures these kernels used to manage process memory layout. Provide tools to introspect into running guests and extract the current process' memory map in Linux

and Windows so that a given address could be identified by object file and symbol name (for instance `write@/lib/libc.so +0x0`).

- Designed a custom hypervisor that provided physical memory management and access to hardware virtualization extensions (Intel VMX).
- As part of the hypervisor project, assisted in the transformation of C code for use in an FPGA that sat on the front side bus.
- Designed a distributed communication layer based on the Map Reduce algorithm that allowed a user to analyze data from multiple appliances in an efficient manner.
- Created an embedded linux distribution that included our custom code and was targeted at removable compact flash "Identity Cards", while taking advantage of our 64-bit cpu and many-GB appliance hardware.
- Taught a weekly class on hacking, covering topics from buffer overflows, shellcode authorship, string injection (including SQL injection), race conditions, cryptography, discovery, and stealth.

- **ClearPath Networks**—El Segundo, CA

*July 2006–January 2007* ClearPath Networks creates an embedded linux appliance that provides firewall, anti-virus, content filtering, and intrusion detection. The devices are remotely configured using a web app.

- Designed a new hardware platform using hardware encryption, reducing production costs by more than 50%.
- Created the embedded linux distribution used on the appliances, and setup the tool chain required to add code to the new hardware platform.
- Contributed to Busybox (an open source application) by adding applets for `ntpcient`, `dhcprelay`, and `arp`.
- Improved Busybox applets `http` and `ifupdown` (added support for vlans).

- **Applied Minds**—Glendale, CA

*August 2005–July 2006* Applied Minds is a think tank that performs engineering research for governments and large corporations. While at AMI, I focused on the distributed database project, which was a parallel system to store structured data with a target capacity of 10 petabytes.

- Developed a b-tree based indexing algorithm (with inspiration from two different published algorithms) to optimize for space while retaining speed. The resulting index could search 2 trillion entries with only three disk reads. Each index is self contained within a single file, and a series of indexes could be written to a raw disk partition using a simplistic directory structure at the head of the volume.
- Created the first distributed cluster for this database, including the implementation of cluster management tools specific to the database, adding cross platform support, and implementing package management. Performed stress and performance tests.
- Designed and implemented the configuration source daemon, which monitored and configured nodes. This added self configuration, self healing, and fault tolerance to the system using zeroconf technology.
- Designed and implemented two database client libraries (in C and pure Java).

- Oversaw the implementation of the fishbowl distributed computing center. This center housed the various test clusters we created at Applied Minds.
- Implemented a triple store (aka Semantic Web in internet parlance) for the United States Air Force.
- Was involved in planning for a UAV (unmanned aerial vehicle) project for the United States Air Force.
- Was involved in the design of an autonomous robotic platform designed to explore artificial life.

- **Navitouch**—Grand Terrace, CA

*June 2003–August 2005* Navitouch created and deployed an embedded linux platform that displayed MPEG video and interactive content on a touch screen. This system was at one time deployed in over 150 Circle K stores in the Los Angeles area.

- Created two linux kernel drivers for the USB touch-screen and USB magnetic card reader.
- Created video player software (based on xine lib) that would take advantage of our hardware MPEG acceleration. Converted this player to a thread safe mozilla plugin.
- Created watchdog systems to self-repair or reboot if failures occur, automated the deployment of ads and collection of report data to a central server, created field automation interfaces, and made the systems otherwise independent.
- Created real time traffic maps based on information from the State of California. As part of this project, I created tools to convert between pixel coordinates and GPS coordinates given three known points, accounting for the unknown manifold transform performed by the map maker in order to place the map in 2D.
- Reverse engineered protocols used by our cellular modem in order to improve functionality under linux. Identified a bug in Verizon Wireless' tower software and provided them with feedback and other assistance to get the bug fixed.

- **Self Employed**—Los Angeles, CA

*June 2002–August 2005*

- Created a proof of concept network intrusion detection system for a computer security firm. The system uses finite state automata to achieve throughput performance 27 times greater than conventional systems.
- Created an embedded linux VoIP router / firewall for use in a city wide wireless voice / data network deployed in Iraq.
- Performed security audits and penetration tests for various clients, focusing on web applications and SQL injection. Performed network forensics for a large law firm in downtown Los Angeles.

- **Quisic, Inc.**—Marina Del Rey, CA

*March 2000–June 2002* Quisic was an online learning company. My role in this company changed from lead programmer at the beginning to chief engineer (with 40 employees under me).

- As Chief Engineer I was involved in three acquisitions – as purchaser twice, and purchasee once.

- As Director of Technology I managed a group of eight programmers and system administrators, and a budget of 2.3 million dollars.
- Re-engineered the hosting and Learning Management System from a monolithic system to a load-balanced redundant system. Improved performance on comparably priced hardware by 1500%, while eliminating 1.2 million dollars of yearly expense, and achieving a system capable of 99.99% uptime.
- Created a content management system for use by our professors and other learning professionals. This project was completed on time and \$750,000 under budget.

- **TeeTimesOnTheInternet.com**—Thousand Oaks, CA

*Chief Technologist: October 1999–March 2000*

- **Transamerica**—Los Angeles, CA

*Lead Programmer: 1997–October 1999*

- **GTE**—Thousand Oaks, CA

*Consultant Programmer: 1996-1997*