Brian C Gerard
3629 Dewing Drive
Raleigh, NC 27616

https://www.linkedin.com/in/briangerard
https://github.com/briangerard
bgerard@gmail.com • 919.862.6825

Summary

I am a technical leader with a diverse repertoire and strong focus on security and automation. I enjoy training and mentorship, have spoken at conferences and user groups, developed and delivered technical training, and led workshops.

18 years in system administration and operations, 13 years in security (mostly focused on abuse prevention), and 10 years in software engineering enable me to bring a uniquely holistic approach to the solutions I create, incorporating the best practices from multiple disciplines and delivering products which are robust, performant, and maintainable. Since I readily engage with people across all levels of the organization, I shepherd my projects from proposal to design, through management buy-in, all the way to implementation and deployment.

- **Languages:** Expert in Perl, Bourne/Bash/Korn shell scripting; professional experience in C, C++, with some in Ruby and PHP; most of my current personal project work is in Go and Python
- **Debugging:** gdb, gcore, strace, ktrace, truss
- **SDLC Tooling:** Jenkins, git, Subversion, CVS, Make, Rake, Jira, Bugzilla, Redmine
- **Agile:** Scrum, Kanban, hybrid methodologies
- **DevOps/Virtualization:** Experience with development and deployment using Puppet and Ansible, and Vagrant with VirtualBox, Qemu/KVM, and VMWare
- **System Performance/Monitoring:** sar, iostat, vmstat, netstat, nagios
- **Systems/OSes:** 10+ years managing hundreds of Unix servers spanning geographic regions, primarily on Linux, FreeBSD (4-9), and Solaris (2.6-9).

Professional Experience

TIAA *(2017-Present)*

SENIOR SECURITY ENGINEER (CONTRACT)
As lead automation engineer and developer for the team, I designed, built, and maintain a Bash and Perl based deployment system which installs and configures the BoKS system on our servers. In parallel, I created a Puppet module to integrate with the TIAA infrastructure in order to facilitate a more robust and reliable roll-out and maintenance, personally leading the deployment on over 6,000 servers in multiple environments.

I designed and developed several administrative software libraries and applications, including:

- A RESTful webservice implemented in Ruby and Sinatra, providing a backend host management interface for the build team. This allows them to automatically register newly-built hosts into BoKS, manage aspects of their lifecycles, and remove them when they are retired from service.
- An ETL application which loads BoKS data into ServiceNow for our user access request forms, and other ETL applications which load data from external sources into our systems.
- An automated user termination system which integrates with a number of other TIAA systems.
- A suite of tools and libraries which abstract and homogenize the management of the BoKS infrastructure and its underlying data according to specified business rules.

I brought git into the team's technology stack, and developed and continue to deliver training for the team on its use. I have developed and delivered training on scripting and automation, as well as the various software solutions I have written.

WELLS FARGO, INC. *(2015-2016)*

SENIOR SECURITY ENGINEER (CONTRACT)
Contract role as a member of the security DevOps team, targeting the upgrade and implementation of Active Directory authentication and authorization of Linux services through BoKS for 6,700 storefront Linux servers and 5,000 general use Linux servers, serving approximately 70,000 end-users. Wrote integration scripts in Linux using Perl and Bash, using MySQL as the database back end. I contributed to the reporting, audit, and

monitoring systems, and wrote a task management system for a project that needed a bespoke solution.

WEBASSIGN, INC. ***(2013-2015)***

STAFF SOFTWARE ENGINEER, SECURITY STEWARD

I designed, architected, and developed the initial revision of the system which currently deploys WebAssign's applications into the development, QA, and production environments. I led the Platform Engineering team through the next several revisions of the system, expanding and abstracting its capabilities. The system is written using a combination of Ansible and scripting (Perl/shell), driven from the command line, from Jenkins, and via a graphical interface using AngularJS fronting Ruby on Rails.

Concurrently serving as Security Steward for the company; in this role:

- Found and fixed a number of application security holes in our products (SQLi, XSS, CSRF).
- Provided architectural guidance and code reviews to the engineering teams.
- Kept upper management apprised of the latest relevant security bulletins, CVE's, etc, and fixed and/or supervised the teams who fixed emergent vulnerabilities (among them, HeartBleed and ShellShock).

Other projects include:

- Developed an in-house monitoring solution for our development and QA systems, filling visibility gaps in the main system until a final monitoring solution could be deployed.
- Created and delivered a class on Bash scripting and command line usage to the Engineering organization. I have since delivered that training (and led a follow-on half day workshop) to the Triangle Linux Users Group. Slides and other materials are available at: https://github.com/briangerard/bash_class

YAHOO!, INC. ***(2005-2013)***

ABUSE/SECURITY SOFTWARE ENGINEER ***(2008-2013)***

I developed three separate training courses on the abuse defense frameworks at Yahoo! and delivered them on a quarterly basis to engineers from across the company. These were made a part of the standard on-boarding curriculum for new engineering hires. I presented at internal and external conferences, arranged speakers for Yahoo!'s annual Security Week, and represented Yahoo! for recruiting at college events.

Working with another engineer on the team, we data mined logs from a major botnet attack against multiple Yahoo! properties and discovered novel characteristics of the traffic. Using these results, we designed and built a new botnet defense system. Using similar techniques, I delved into our CAPTCHA data on the Hadoop grid and developed a new defense against a previously unknown attack vector.

Leadership roles:

- Initiated the program to architect our new abuse defense framework, and designed, contributed to, or consulted on almost every component of the systems that now make it up.
- Created the Statement of Work and served as Technical Liaison for a major rewrite project we outsourced to a contracting firm in India.
- Managed the sustaining engineering (SWAT) group within the Abuse Engineering organization, leading the development sprints, hiring new team members,and defining the direction for the group.
- Coordinated abuse defense integration across all participating properties for World IPv6 Day (2011/06/08) and World IPv6 Launch Day (2012/06/06). While managing the development, testing, and deployment of the updated platforms, I worked with teams across the company to ensure we were ready when the world went live.

ABUSE DEFENSE/SECURITY SPECIALIST ***(2005-2008)***

I designed, tuned, and coordinated the deployment of abuse defenses for many of Yahoo!'s premier properties, including Mail, Finance, Ad Systems, Answers, and Shopping. I wrote custom Perl scripts to handle the data analysis needed for effective design, and directly interfaced Perl with our internal tool suite, enabling us to further customize the defenses.

As the technical lead for the team, I trained all new hires and provided ongoing mentorship on the more complex issues and attacks that we handled. I implemented several subsystems in our abuse feedback tracking system and account deactivation system, allowing Yahoo! properties to automatically disable abusive accounts as needed. I wrote tools that the team still uses to effectively analyze operational issues.

I took over custodianship of Yahoo!'s internal network database (dbm-based) and brought the build time down, from days to under an hour, by automating many of the data modifications and complex cross checks between the diverse sources that had been handled manually; such as security level validation and subnet overlap detection and splitting. I organized the interdepartmental team and drove the project which migrated custodianship of this critical system to its current owners.

MIRAPOINT, INC. ***(2004-2005)***
SENIOR TECHNICAL SUPPORT ENGINEER
In addition to system analysis and live online troubleshooting of customer production servers, I created scripts to manage and analyze the large volumes of incoming system diagnostic data. This allowed us an enterprise wide view of customers' Mirapoint systems (dedicated FreeBSD-based email appliances), which in turn provided a means of proactive troubleshooting and sizing prediction.

I was entrusted with administrative login access to customers' live production servers via proprietary configuration interface and shell access. The debugging process included process tracing, and log, network, and core dump analysis, and required deep knowledge of TCP/IP, SMTP, LDAP, IMAP, and DNS.

NEOFORMA, INC. ***(2002 - 2004)***
UNIX SYSTEM ADMINISTRATOR
I was Operations Lead on a range of projects, including the migration of our SAN and NAS from EMC to HDS, multi-domain NIS/netgroup setup in three datacenters, engineering Perl-based failover solutions (LAN and WAN) for various suites of applications, and writing a centralized log rotation and archival system for a variety of servers. I led three to six engineering projects annually, and fostered interdepartmental cooperation between the Engineering, DBA, System Administration, and Production Support teams. I documented and led the final deployment of those projects into the production environment.

I managed multiple Veritas clusters (VCS 3.5), Linux DNS and sendmail servers, and a variety of networking equipment (Cisco 5500/6500 switches, PIX firewalls, and 25XX/26XX routers). I administered our SAN (first EMC/McData, then HDS/Brocade) and NAS (first EMC Celerra, then Veritas clustered Sun 420Rs; a NetApp Filer throughout), and managed NIS for 3 sites and 120+ servers with over 3000 users.

COLLECTIVE TECHNOLOGIES, INC. ***(2000 - 2002)***
CONSULTANT
In addition to the work I performed at my client sites, I gave technical assistance to junior members and provided leads and sales engineering support for our sales staff.

NEOFORMA, INC.

Besides the project work and technical tasks listed in the Neoforma section (above), I worked with management to expand Collective's consulting presence on several occasions, meeting Neoforma's challenges as they arose.

DIGEX, INC.

I was solely responsible for the IT needs of three west coast facilities. I managed everything from desktop phones (punchdown through switch configuration), to NT domain administration, desktop builds, and network troubleshooting (on the switch, and NT and Solaris workstations). I brought the IT inventory under control, and hired, and trained a full time employee to replace me at the end of the contract.

Previous roles

- **RESONATE, INC.** ***(1998 - 1999)*** - SOFTWARE QA ENGINEER, AND SYSTEM ADMINISTRATOR
- **ASSET CONSULTING GROUP, INC.** ***(1996 - 1998)*** - SYSTEM ADMINISTRATOR AND WEBMASTER

Affiliations

TRIANGLE LINUX USERS GROUP (www.trilug.org)
(2015 - Present) CHAIR; ***(2014 - 2015)*** VICE CHAIR
I organize and help facilitate our meetings and workshops, arrange speakers, and collaborate with other area organizations. I manage the Steering Committee's projects, which have included multiple venue changes.