Kevin M. Gallagher
437A Arlington St. • San Francisco, CA 94131 • (781) 771-7379 •
kevingallagher@gmail.com • Twitter: @ageis

Recent Work History

The Calyx Institute – January 2018 to Present – calyxinstitute.org

> Part-time sysadmin. Helping a small privacy-focused non-profit with minor infrastructural needs on an ad-hoc and hourly basis. Founded as a service provider in 1995 by one who later became the first person to constitutionally challenge what are known as National Security Letters (NSLs), The Calyx Institute runs a public Jabber server, maintains several high-bandwidth Tor relays, and provides several other services to its membership.

Cloudflare – August 2016 to September 2017 – cloudflare.com

> Systems Reliability Engineer. Helping a respectable portion of global internet CDN and DNS infrastructure run reliably.

• Worked on-call rotation, debugging issues across the full stack in nearly ~120 points of presence
• Provisioned new datacenters and released new versions of core software to them
• Developed and deployed tools for measuring the latency of DNS zone propagation
• Contributed ideas and proposals to other teams on security and performance issues
• Triaged alerts, wrote incident report(s), updated references and tuned thresholds to reduce noise
• Participated in a project to make tools and manual SRE processes more efficient
• Fulfilled technical requests from other teams as well as customers, often related to the SSL pipeline

Zcash Company – August 2016 to June 2017 – z.cash

> DevOps Engineer. Managing infrastructure and operational security for Zcash, a decentralized and open source cryptocurrency that aims to set a new standard for privacy through the use of groundbreaking cryptography.

• Contributed to the design of the zero-knowledge parameter generation ceremony or “trusted setup”
• Designed a fully deterministic build process and environment using Gitian
• Assisted with static analysis and fuzzing of software to mitigate C/C++ memory safety issues
• Maintained and updated the Python-based continuous integration system known as Buildbot
• Packaged the software for Debian, also set up an apt repository and binary releases using off-line, air-gapped processes for signing software
• Designed monitoring and alerting systems with metrics and log aggregation / parsing (using Prometheus, Grafana, and ELK) for the Zcash blockchain, with the ability to detect chain forks and malicious network activity
• Responded to security incidents and concerns as needed, identifying a critical segfault-causing bug w/ gdb
• Implemented multi-factor authentication at an organizational level via TOTP and U2F
• Set up a DNS seeder to bootstrap the network and help peers find each other
• Automated the entirety of company infrastructure where no version control previously existed

Freedom of the Press Foundation – March 2014 to July 2016 – freedom.press

> Systems administrator. Deployed, managed and fully automated numerous services and infrastructure, both internal and public-facing, at a high level of security for a non-profit that supports transparency journalism. Also contributed extensively to the SecureDrop open source whistleblower platform which is used by news organizations worldwide.

• Set up self-hosted and secure collaboration solutions instead of relying upon third-party service providers
• Wrote custom PHP and JS code to integrate payment processors with Drupal and CiviCRM
• Published blogs on assorted topics & assisted the Executive Director with general operations management
• Edited and contributed to guides and trained journalists and other members of the public on encryption
• Built the SecureDrop support portal, making improvements to a custom OpenPGP plugin for Redmine. Also built a monitoring system for Tor hidden services, provided technical support to users and administrators, created and maintained the apt software repository for SecureDrop, and helped automate instance setup
• Surveyed news organizations for their use, and encouraged adoption of HTTPS and STARTTLS
• Wrote scripts for configuring the Tails amnesic operating system for use with SecureDrop
• Developed documentation for running kernels w/ grsecurity/PaX & using YubiKeys with SSH+GPG
• Wrote Ansible roles, Logstash filters and grok patterns covering all services and servers for their ELK deployment

Library Freedom Project – February 2015 to Present – libraryfreedomproject.org

> Part-time sysadmin. Maintaining the website and email server for a project to make real the promise of intellectual freedom and privacy within libraries, including by encouraging them to run Tor relays.

Transparency Toolkit – July 2014 to Present – transparencytoolkit.org

> Part-time sysadmin. Managing servers and helping with research for an organization that gathers data on surveillance and human rights abuses and writes software to analyze it. Assisted deployment of code for crawling, scraping, parsing, visualizing and analyzing massive datasets.

• Helped launch the Snowden document search, Surveillance Industry Index, and ICWATCH websites with high availability
• Participated in strategic partnerships with Privacy International and Courage Foundation et al.
• Leveraged container orchestration and an ElasticSearch cluster to host multiple instances of the same complex software written in Ruby
• Mitigated DDoS attacks against our sites such as a mirror of the Hacking Team leak

left-click – September 2012 to December 2014 – www.leftclick.us

> Sysadmin. Managing networks, servers and phone systems for two retail locations plus a Linux-based point-of-sale system installed at a local supermarket. Lead technician on several projects for select clients, including computing clusters, thin clients, VoIP, legacy websites, e-mail migrations, remote backups, information security and compliance programs, VPNs and wireless access points.

Last Call Media – September 2012 to December 2014 – lastcallmedia.com

> Sysadmin. Related to above as another division of the company. Managing medium-sized IT infrastructure in support of Drupal web development, including numerous servers on which hundreds of sites are hosted.

• Assured security, reliability & performance of networks and daemons and troubleshooted various hardware and software issues. Worked extensively with Git, Bash scripting, PHP and MySQL.
• Performed migrations, deployments and updates of mostly Drupal-based websites and VPSes.
• Responsible for setup, configuration and maintenance of internal company infrastructure: Asterisk PBX / VoIP phones, environment synchronization with Puppet, periodic backups via BackupPC, monitoring with Nagios, Redmine for project management, and network routers + devices. Ensured comprehensive documentation.
• Also assisted with the continuous integration environment for staging and development based on Sismo.

Education

University of Massachusetts, Amherst – B.A. in English, 2012

Certifications

Red Hat Certified Sysadmin – 120-126-396	CompTIA Linux+ – QDSZ76CC9CRES4RP
LPIC-1 – LPI000264195	Novell Certified Linux Administrator – 10192939

Advocacy

Free Barrett Brown – September 2012 to July 2015 – freebarrettbrown.org

Director and Founder. Support network, not-for-profit advocacy organization and legal defense fund formed for the purpose of assisting a prominent imprisoned journalist and internet activist. In charge of all fundraising, public relations, social media and outreach.

Computer Skills and Experience

Programming: Python, Bash, PHP, HTML/CSS/JavaScript, Perl, *some* Ruby on Rails, *some* C/C++
Operating Systems: Linux, Windows, Mac OS X, FreeBSD, Android … also Qubes, Tails, and Subgraph
Various Unix: Apache, Postfix, Dovecot, Samba, nfs, Squid, Varnish, HAProxy, MySQL, PostgreSQL, git, GNU coreutils, iptables, Asterisk, OpenVPN, Salt Stack, Nagios, nginx, Tor, regex, LUKS/cryptsetup/dm-crypt, virtualization (KVM, Xen, VirtualBox, VMWare, Proxmox, Vagrant), containerization (Docker, LXC), kernel and filesystem configuration, LTSP (Linux Terminal Server Project), Ansible, grsecurity/PaX, GnuPG, OSSEC, ELK (ElasticSearch, Logstash and Kibana), Riemann, Snort, ModSecurity, Serverspec/Testinfra, osquery, Prometheus, Grafana, mtail, cadvisor, Buildbot, Travis, Jenkins, dnsmasq, Unbound, gdb, systemd, IPMI, AppArmor, SELinux, BIND, BIRD, rsyslog, OpenSSH, OpenSSL, ejabberd, Prosody, UnrealIRCd, Nessus, Metasploit, Acunetix, Burp Suite, Shodan, Wireshark, pfSense/OPNsense, OpenWrt/Tomato/DD-WRT, IPsec/strongSwan, LDAP, RADIUS, seccomp-bpf, BIRD, AFL (american fuzzy lop), Coverity Scan, Nmap, sqlmap, hashcat/John the Ripper, Kismet/Aircrack-ng, Ettercap, mitmproxy, *some* Puppet and Chef, dpkg, aptly, TPM (Trusted Platform Module), CHIPSEC, auditd, cPanel, Avahi/Zeroconf/Bonjour, miniDLNA, npm/nodejs, YubiKey, Moloch, Android SDK, PPTP, L2TP, ffmpeg, DNSSEC, DANE
Cloud: Amazon Web Services (EC2), DigitalOcean, Google Cloud Platform (GCE), Microsoft Azure, Rackspace, Gandi, Linode, OVH, UnitedLayer, iPredator
Web: WordPress, Drupal, CiviCRM, MediaWiki, ownCloud, Redmine, GitLab, Piwik
Learning about: Kubernetes, Mesos, CoreOS, OpenStack, Kafka, Solr, SIMP, OpenSCAP, Sysdig, eBPF, SystemTap, Dtrace, Zabbix, Heka, Bosun
Interested in: monitoring, automation, log aggregation, vulnerability assessment, system security and hardening, alerting, intrusion detection, file and platform integrity, metrics visualization and analytics, daemon configuration, application deployment, transport layer security, privacy and transparency

Publications

The Daily Beast, The Guardian, Huffington Post, VICE Motherboard, New York Observer, Daily Dot, The Mass Media, The Daily Collegian, Nexus: The International Henry Miller Journal

Presentations

Hackers on Planet Earth, Mozilla Privacy Lab, Computers Freedom & Privacy, NERDSummit, RightsCon, Bay Area Drupal Camp