

KEVIN GALLAGHER

Professional Linux systems administrator / DevOps / SRE / security engineer

@ kevingallagher@gmail.com 📍 United States of America 🔗 <https://cointel.pro> 🐦 @ageis
in [linkedin.com/in/kevinmichaelgallagher](https://www.linkedin.com/in/kevinmichaelgallagher) 🐙 github.com/ageis 🔑 0xB604C32AD5D7C6D8



RECENT WORK EXPERIENCE

Senior Systems Engineer

Pandora Media, Inc.

📅 April 2018 – December 2018 📍 Oakland, CA

- Wrote Ansible roles covering a diverse environment of ~8,000 machines running different versions of Debian. Developed a callback plugin to provide greater visibility of errors in automation code. Migrated various components out of dpkg/Jenkins and into Ansible
- Deployed Prometheus exporters, alerts and dashboards to monitor the state of LDAP, BIND DNS and the Logstash/rsyslog pipeline
- Developed tooling to share the HashiCorp Vault master key between several team members utilizing Shamir's Secret Sharing
- Coordinated the updating of NTP configurations and a 2s leap second correction without disruption
- Managed global upgrade of Java JDK which fixed TLS handshakes w/ advertisers and restored revenue. Consulted on PKI and compliance
- Participated in the on-call rotation, investigated issues across the full stack, and handled tickets from other departments: including imaging, provisioning, DNS updates, access requests, etc.
- Built a new mail server to replace aging infrastructure. Also helped migrate Nagios and Alertmanager notifications into ELK to reduce e-mail volume

Systems Reliability Engineer

Cloudflare

📅 August 2016 – September 2017 📍 San Francisco, CA

- Worked on-call, debugging issues across the full stack in nearly ~130 points of presence. Responsible for availability of 10% of internet
- Provisioned new datacenters and released new versions of core software to them
- Developed and deployed tools for measuring the latency of 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

DevOps Engineer

Zcash Company

📅 August 2016 – June 2017 📍 z.cash

- Contributed to the design of the zero-knowledge parameter generation ceremony or "trusted setup"
- Designed a fully deterministic build process and environment
- Assisted with static analysis and fuzzing of software to mitigate C/C++ memory safety issues

EDUCATION

B.A. in English

University of Massachusetts, Amherst

📅 2012

CERTIFICATIONS

Red Hat Certified Sysadmin | 120-126-396

CompTIA Linux+ | QDSZ76CC9CRES4RP

LPIC-1 | LPI000264195

Novell Certified Linux Administrator | 10192939

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

TECHNICAL INTERESTS

monitoring and alerting

automation

log aggregation

vulnerability assessment

system security and hardening

intrusion detection

file and platform integrity

metrics visualization and analytics

daemon configuration and application deployment

transport layer security and encryption

privacy and transparency

PROGRAMMING

Python

Bash

PHP

HTML/CSS/JavaScript

Perl

some Ruby on Rails, Go, and basic C/C++

- Maintained and updated Python-based continuous integration system
- Packaged the software, 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 & 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, once identifying a critical segfault-causing bug (remote DoS) 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

Systems Administrator

Freedom of the Press Foundation

📅 March 2014 – July 2016 📍 freedom.press

- 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 hardened Linux kernels w/ grsecurity/PaX and using YubiKeys with SSH+GPG
- Wrote Ansible playbooks, Logstash filters and grok patterns covering all services and servers for their ELK deployment

PART-TIME ROLES

Library Freedom Project

📅 February 2015 to Present 📍 libraryfreedomproject.org

- Maintaining the website and email server for a project to make real the promise of intellectual freedom and privacy within libraries.

Transparency Toolkit

📅 July 2014 to Present 📍 transparencytoolkit.org

- Managing servers and helping with research for a group that gathers data on surveillance and human rights abuses using open-source intelligence and then writes analytics software to present it.

The Calyx Institute

📅 January 2018 to Present 📍 calyxinstitute.org

- Helping a small privacy-focused non-profit with minor infrastructural needs on an ad-hoc and hourly basis.

PRESENTATIONS

Hackers on Planet Earth

Mozilla Privacy Lab

Computers Freedom & Privacy

NERDSummit

RightsCon

Bay Area Drupal Camp

ADVOCACY

Free Barrett Brown

Founder and Director

📅 9/2012–7/2015 📍 freebarrettbrown.org

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.

CryptoParty

Enthusiast and Trainer

📅 Since October 2012

Involved with the Massachusetts Pirate Party in training journalists, lawyers, human rights activists, and other interested members of the public to secure their digital communications and data. Presented workshops on various well-known privacy and encryption tools.

MISC. TOOLING

Ansible • ELK (ElasticSearch, Logstash & Kibana)
 Prometheus • Grafana • osquery • Kolide Fleet
 Docker • Apache • nginx • Postfix • Dovecot • auditd
 dnsmasq • BIND • Unbound • MySQL • PostgreSQL
 OpenSSH • OpenSSL • Squid • Varnish • HAProxy
 Tor • GnuPG • OSSEC • Wazuh • grsecurity/PaX
 AppArmor • LUKS/cryptsetup • GNU coreutils • make
 Meson • Ninja • git • systemd • iptables • rsyslog
 dpkg • Nagios • Riemann • OpenVPN • L2TP • PPTPd
 OpenLDAP • Samba • KVM • Xen • VirtualBox
 VMWare • Proxmox • Vagrant • LXC • Nessus • aptly
 nfs • Salt Stack • IPMI • RDP/VNC • AFL • Asterisk
 Jenkins • Buildbot • pfSense/OPNsense • eBPF • gdb
 IPsec/strongSwan • Wireshark • LTSP • Coverity Scan
 ModSecurity • Sonatype Nexus • PAM • Android SDK
 Metasploit • ejabberd • UnrealIRCd • BIRD • SNMPd
 OpenSCAP • SIMP • FreeRADIUS • nodejs/npm/yarn
 Kubernetes • Mesos • Nomad • HashiCorp Vault • Consul
 AWS/EC2 • Google Cloud • DigitalOcean • Microsoft Azure
 Rackspace • Linode • Gandi • OVH • UnitedLayer

and more...