Susan E. Sons

Information Security and Software Engineering

Phone: (812) 272-7394 Email: sons@security.engineering

WORK

Senior Systems Analyst 2014-present

Center for Applied Cybersecurity Research (CACR), Indiana University

- As a member of the Center for Trustworthy Scientific Cyberinfrastructure (CTSC), engaged with NSF-funded projects and facilities, including DKIST, LSST, HUBzero, Gemini, PerfSONAR, and OOI, to meet their particular information security needs in areas including training, program development, code analysis, evaluation of specific technologies, risk assessment, and implementation of specific controls.
- Identified the crisis state of the NTP software project and spearheaded an experimental engagement format in which CTSC partnered with the nonprofit ICEI to migrate the NTP code base to an accessible source code repository, fix some of its security vulnerabilities, and provide the build/test infrastructure and documentation needed for further development and hardening. In the end, this engagement left NTP with a solid start for a more secure future, and community efforts to maintain and iterate on this positive change are being funded by Linux Foundation's Core Infrastructure Initiative.
- Working with Open Science Grid (OSG) to improve their security posture by performing a review of their cybersecurity program, improving certificate issuance mechanisms, and building out new software assurance mechanisms in preparation for the planned handoff to CACR of OSG's programmatic and operational cybersecurity responsibilities in 2017.
- Co-authored the *Guide to Developing Cybersecurity Programs for NSF Science and Engineering Projects*.
- Served on the planning committee for the 2015 and 2016 NSF Cybersecurity Summits as CFP Lead.
- Designed and co-led training on secure software engineering practice at the 2016 NSF Cybersecurity Summit.
- Presented training on Building Cybersecurity Programs for NSF Projects and Facilities at the 2014, 2015, and 2016 NSF Cybersecurity Summits.
- Worked with a team to draft the Cybersecurity chapter of the upcoming revision of the NSF Large Facilities Manual.
- Ran numerous training events for academic, scientific, and other software development communities on: incident response, information security program building, vulnerability management, security hygiene, and secure software development practices.
- Assisted in leading a Rust systems programming tutorial at OSCON 2016.
- Managed two graduate research assistants.
- Served on the Program Committee for the 2015 CACR Cybersecurity Summit.
- As a member of the information security team on the DHS-funded Software Assurance Marketplace (SWAMP) project, advise the principle investigators on information security policy, perform routine security audits, select security controls, coordinate mock security incident exercises, refine the cybersecurity program, respond to live incidents, and provide cybersecurity insight to the SWAMP's software development team.

Information Security Officer, Emeritus 2015-present

NTP Security Project

- Following completion of the successful NTP Rescue project launched from within CTSC, served under Linux Foundation's Core Infrastructure Initiative to support the resulting fork, NTPSec, as Information Security Officer.
- Led incident response.
- Provided information security training to developers.
- Aided developers in assessing and patching security vulnerabilities in NTPSec, as well as in communicating with responsible disclosers.
- Acted as a liaison between the NTPSec project and scientific computing and infrastructure stakeholders.
- Stepped down as ISO in Q2 2016, at which time I was awarded an emeritus position in recognition of my continuing advocacy and provision of expertise to the project.

Developer, Project Manager, Consultant, Instructor 2007-2014

Self Employed

- Wrote code ranging from simple Drupal modules to more complex standalone webapps, deployment tools, and so on.
- Worked with a wide array of technologies, including Drupal, PHP, Python, Apache, Nginx, Mysql, PostgreSQL, MongoDB, Pyramid, shell scripting, git, svn, cvs, Varnish, php-fpm, etc.
- Scoped and managed projects ranging from simple small business web sites to complex integrations and web presence migrations.
- Managed several complex recoveries where network-facing applications were exploited, and proper mitigations had not been in place. Took ownership of analysis and recovery operations, as well as recommending and/or implementing improvements to mitigate risk of and detect future incidents.
- Provided training on programming languages, tools, CMSes, and frameworks as well as secure coding practices.
- Created development, documentation, and quality assurance workflows suitable for the in-house staff who would pick up from where I left off, and provided documentation and training for those developers on both the system and the workflows in place.
- Managed subcontractors and/or clients' in-house IT personnel as needed.

Community Manager 2011

Stack Exchange (Stack Overflow)

- Worked with a team to oversee over twenty web site communities, including StackOverflow.com, SuperUser.com, and ServerFault.com.
- Provided mentorship and guidance to site moderators.
- Helped to design and oversee gamification aspects of the various sites, i.e. points awarded or deducted for various behaviors and the escalating ban system.
- Helped to grow sites through promotional activities, and facilitated the community-driven site creation process.

Developer 2004-2005

Sytex Southwest

- Developed web sites and applications for clients.
- Answered RFPs for government client projects.
- Floated to other departments, gaining experience in system administration, networking, and security (both technology and policy/procedure).

VOLUNTEERISM

Director 2015-present
Internet Civil Engineering Institute

- Promoted by the board from Systems Administrator after Eric S. Raymond stepped down.
- Conceived of and implemented the Information Security for Shared Infrastructure (ISSI) program, through which ICEI offers information security expertise and manpower to open source infrastructure software projects that need it.
- Led a cooperative engagement (”rescue”) of the NTP software project under this program in conjunction with Indiana University and the National Science Foundation’s Center for Trustworthy Scientific Cyberinfrastructure.
- Currently expanding ISSI through training of new software security experts and engagement with additional open source infrastructure projects.
- Responsible for communication with ICEI’s Oversight Board, for recruiting and managing volunteer staff, and for developing programs to support ICEI’s mission.
- Primary point of contact for press, large donors, and partner organizations.

Project Lead 2015-present
New Guard

- Running an informal group to provide cross-mentorship among early- and mid-career technologists who wish to become infrastructure software maintainers, and matching them with experienced infrastructure software maintainers for training and mentorship.

Systems Administrator 2012-2015
Internet Civil Engineering Institute

- Managed the organization’s server infrastructure including email, web server, git server, and various web applications.
- Spearheaded planning for future infrastructure needs, especially with regard to scalability and support for data gathering from projects like Kronos – which seeks to place independent GPSr-based timing hardware at as many internet endpoints as possible – and the internet traffic mapping projects to follow.
- Worked with the organization’s Board of Directors to plan and implement fundraising and outreach projects that make ICEI’s mission possible.

President, Founder 2010-2011
Drupal Indy Group

- Founded the organization with a group of fellow Drupal profressionals to expand work we’d begun as an informal collective.
- Managed fundraising.
- Planned and managed events from small meetups to medium-sized (up to 1k attendees) conferences.
- Provided technical content and training for events.

Abusive Hosts Blocking List Technical Staff 2004 - 2009
Summit Open Source Development Group

- Created and maintained automated tools for analysis and reporting of patterns and trends in honeypot email.
- Created and maintained automated tools for tracking sources of abuse tools so that they can be reported to hosts and removed.

- Managed additions to and removals from our DNSBL per AHBL's policies.
- Acted as a liaison to abuse departments at a number of service providers, and to staff of other blocklists and abuse-related organizations.

Freenode Network Staff, Developer 2003-2006
Peer-Directed Project Center

- Helped to maintain the existing Hyperion IRCd codebase pending migration to a more stable system.
- Oversaw development of a new services suite so that freenode could be migrated to a standard IRCd without loosing features the community depended on.
- Worked on methods and code for the automated detection of botnets and other sources of automated and directly human-generated abuse on the network.
- Aided in the design and improvement of abuse-mitigation tools and abuse response protocols.
- Acted as a liaison to law enforcement on abuse-related matters when one was required.

PUBLICATIONS

Under the Sink LinuxJournal, Dec 2015 to Present
A regular column on infrastructure software and information security

Guide to Developing Cybersecurity Programs for NSF Science and Engineering Projects CTSC, 2014
http://trustedci.org/guide

EOF: Girls and Software LinuxJournal, Feb 2014
http://www.linuxjournal.com/content/girls-and-software

The Definitive Guide to Drupal 7 Apress, 2011
Co-Authored under a previous name: Susan Stewart

The Edubuntu Cookbook Canonical, 2006
Co-Authored under a previous name: Susan Stewart