Susan Sons

📞 +1 812 272-7394
✉ sons@security.engineering
🖳 http://security.engineering

━━━━━ Experience

Mar 2014 –Present **Senior Systems Analyst**, *Center for Applied Cybersecurity Research, Indiana University*.

- Serving as Information Security Officer for Open Science Grid, a DOE and NSF-funded infrastructure project connecting users and organizations throughout the United States with high throughput computing resources.
- Managed several outside project staff—employees of partner institutions who were subordinate members of specific grants or projects—graduate students, and one full-time direct report.
- As a member of the NSF Cybersecurity Center of Excellence, engaged with NSF-funded projects and facilities, including DKIST, LSST, HUBzero, Gemini, PerfSONAR, and OOI, to serve their particular information security needs.
- 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 were then funded by Linux Foundation's Core Infrastructure Initiative.
- 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.

2016 –Present **President**, *Internet Civil Engineering Institute*.

- Created and leading *New Guard*, a mentoring program for the next generation of infrastructure software maintainers.
- Conceived of and implemented a program through which ICEI offers information security expertise and manpower to open source infrastructure projects that need it, and enabled that program's growth through the training of new software security experts and engagement with additional open source infrastructure projects.
- Responsible for communication with ICEI's Board of Directors, fundraising, recruiting and managing staff, and for developing programs to support ICEI's mission.
- Recruited to the position by ICEI's board after serving as the organization's systems administrator since 2012.

2015–2016 **Information Security Officer**, *NTP Security Project*.

- Following completion of the successful NTP Rescue project within CTSC, served the resulting fork, NTPSec, as Information Security Officer.
- Led incident response, and aided developers in assessing and patching security vulnerabilities in NTPSec, as well as in communicating with responsible disclosers.
- Provided information security training to developers.
- Acted as a liaison between the NTPSec project and scientific computing and infrastructure stakeholders.
- Handled succession planning in advance of my eventually moving on from the project, selecting my own replacement and ensuring a smooth transition
- 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.

2011   **Community Manager**, *Stack Exchange*.
- Worked with a team to oversee over twenty web site communities, including StackOverflow.com, SuperUser.com, and ServerFault.com, providing mentorship and guidance to site moderators, and helping to grow user bases.
- 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.

2007–2014   **Developer, Project Manager, Consultant, Instructor**, *Self Employed*.
- 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.
- Wrote code ranging from simple Drupal modules to more complex standalone webapps, deployment tools, and so on.
- 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.
- Managed subcontractors and/or clients' in-house IT personnel as needed.

2003–2006   **Volunteer Freenode Network Staff, Developer**, *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 losing 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.
- Acted as a liaison to law enforcement on abuse-related matters when one was required.

2004–2005   **Developer**, *Sytex Southwest*.
- Developed websites and applications for clients.
- Answered RFPs for government client projects.
- Floated to other departments, gaining experience in systems administration, networking, and security (both technology and policy/procedure).

Publications

Articles.
- **Linux Journal Column: Under the Sink** *covers topics related to infrastructure software and information security, appearing regularly since December 2015.*
- **EOF: Girls and Software** *guest editorial on growing up a girl hacker in the 1990s, appearing in Linux Journal December 2013.*

Books.
- **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*

Other.
- **Guide to Developing Cybersecurity Programs for NSF Science and Engineering Projects** http://trustedci.org/guide