Susan Sons

+1 812 272-7394 • sons@security.engineering
http://security.engineering

Experience

Center for Applied Cybersecurity Research, Indiana University

Senior Systems Analyst *March 2014–Present*

https://cacr.iu.edu

- Currently serving as Information Security Officer for Open Science Grid (https://www.opensciencegrid.org), 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, CTSC (https://trustedci.org), 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.
- As a member of the information security team on the DHS-funded Software Assurance Marketplace (SWAMP) project (https://continuousassurance.org), 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.
- Served on the Planning Committee for the 2015 and 2016 NSF Cybersecurity Summits as CFP Lead.
- Served on the Program Committee for the 2015 CACR Cybersecurity Summit.

Internet Civil Engineering Institute

President *2016–Present*

https://icei.org

- Created and leading *New Guard*, a mentoring program for the next generation of infrastructure software maintainers.
- Conceived of and implemented the Information Security for Shared Infrastructure program (ISSI), through which ICEI offers information security expertise and manpower to open source infrastructure projects that need it.
- Currently expanding ISSI through training of new software security experts and engagement with additional open source infrastructure projects.
- Responsible for communication with ICEI's Board of Directors, for recruiting and managing staff, and for developing programs to support ICEI's mission.
- Primary point of contact for press, large donors, and partner organizations.
- Working with the organization's Board of Directors to plan and implement fundraising and outreach projects that make ICEI's mission possible.
- Recruited to the position by ICEI's board after serving as the organization's systems administrator.

NTP Security Project

Information Security Officer *2015–2016*

https://ntpsec.org

- 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.
- 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.

Internet Civil Engineering Institute

Systems Administrator *2012–2016*

- 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.

Stack Exchange

Community Manager *2011*

http://stackexchange.com

- 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.

Summit Open Source Development Group

Abusive Hosts Blocking List Technical Staff *2004-2009*

- 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.

Self Employed

Developer, Project Manager, Consultant, Instructor *2007–2014*

- 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.
- 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.

Peer-Directed Project Center

Volunteer Freenode Network Staff, Developer *2003–2006*

- 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.
- 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.
- Helped with user service tasks ranging from password resets to channel and cloak management.

Sytex Southwest

Developer *2004–2005*

- 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

- **Postmortem** **Linux Journal, Feb 2017**
  What to do after a security incident.
- **Holy Triage, Batman!** **Linux Journal, Nov 2016**
  Code triage: it's a dirty job, but somebody's got to do it...
- **Security Exercises** **Linux Journal, July 2016**
  A crash course on how to plan effective security exercises
- **Securing the Programmer, Part I** **Linux Journal, May 2016**
  How developers can prevent compromise at their workstations
- **Fast Network Routing, Meet Userspace** **Linux Journal, Feb 2016**
  Interview with Katerina Barone-Adesi about Snabb Switch network toolkit

- **Chain of Custody** — **Linux Journal, Dec 2015**
  Gaps in the chain of code integrity
- **EOF: Girls and Software** — **Linux Journal, Dec 2013**
  Guest editorial on growing up a girl hacker in the 1990s

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** — **CTSC**
  http://trustedci.org/guide

Presentations

This far from a complete list of presentations I have given. Instead, I've attempted to showcase a selection that highlights the variety of talks and trainings I give. If you are interested in a more comprehensive listing, please see http://security.engineering/talks where I am endeavoring to build a library of my past presentations and related materials.

- **Rebuilding a Plane In Flight: Refactors Under Pressure**
  Currently under development, this 3.5-hour training program will first be offered at the OSCON 2017 in Austin, TX (https://conferences.oreilly.com/oscon/oscon-tx/public/schedule/detail/57202). I've spent most of my career refactoring systems and software in various states of crisis, many with critical deployments which could not be taken out of service. This training covers the skills needed to scope, resource, and carry out such projects for maximum effectiveness while mitigating risk to active deployments.
- **Cybersecurity For Journalists Panel**
  Hosted in February 2017 by Indiana University's Media School, this panel gave me the opportunity to join a journalist, an EFF attorney, and a media law professor in educating future journalists and members of the community about how journalists can protect their sources and their stories, the current landscape for journalism and free speech, as well as cybersecurity concerns relevant to the general public and potential leakers/sources. Details are available at http://security.engineering/talks/journalists2017.
- **Saving Time: How a few committed people helped hold up the Internet. . . again**
  Presented at the 2016 O'Reilly Security Conference in NYC, this talk used the rescue of the ailing Network Time Protocol reference implementation as a case study in the impacts of aging, troubled infrastructure software and the lack of skilled maintainers. See https://conferences.oreilly.com/security/network-data-security-ny/public/schedule/detail/53199 for details and a link to slides. Full video is available on O'Reilly Safari.
- **Secure Software Development Best Practices**
  Co-presented with my colleague Randy Heiland at the 2016 NSF Cybersecurity Summit in Washington, D.C. http://trustedci.org/2016summit for details.
- **Developing Cybersecurity Programs for NSF Projects**
  Since my team developed the *Guide to Developing Cybersecurity Programs for NSF Science and Engineering Projects*, the accompanying 4-hour training has been a perennial staple at the NSF's cybersecurity conference. See http://trustedci.org/2016summit, http://trustedci.org/2015summit, and http://trustedci.org/2014summit for details.

- **Saving Time: How a few committed people helped hold up the Internet. . . again**
  Presented at the 2016 O'Reilly Security Conference in NYC, this talk used the rescue of the ailing Network Time Protocol reference implementation as a case study in the impacts of aging, troubled infrastructure software and the lack of skilled maintainers. See https://conferences.oreilly.com/security/network-data-security-ny/public/schedule/detail/53199 for details and a link to slides. Full video is available on O'Reilly Safari.
- **Practical Cybersecurity for Lawyers and Law Firms**
  I co-presented this full-day Continuing Legal Education training event with my colleague, attorney Craig Jackson, in December 2015. While many of the lawyers we worked with had learned about cybersecurity law to varying degrees, almost none had had prior instruction on securing the sensitive information that they and their firms handle as a matter of course every day. See https://cacr.iu.edu/lawyers for details. Full video is available on O'Reilly Safari.

Press

Again, not a comprehensive listing. However, this particular piece includes a video interview that is a quick opportunity to get to know me.

- **NTP: the rebirth of ailing, failing core network infrastructure** by Cory Doctorow
  includes video interview by Mac Slocum at O'Reilly Media
  http://boingboing.net/2016/11/29/ntp-the-rebirth-of-ailing-fa.html