Eleanor Saitta

ella@structures.systems Remote EST/GMT
https://structures.systems Permanent, 2/3 time

As a fractional Chief Security Officer, I build security teams and programs for startups and bring two decades of security experience in architecture, strategy, and governance to companies early in their security journeys. I treat security as a business enabler, not just a risk mitigation process, whether that's making investors comfortable enough to add $150m to an existing $350m funding round, re-architecting a drug discovery company's wet lab robot controllers so they can be treated like cloud resources, or showing principal engineers that for the first time in their career, security can be an active partner they look forward to working with. Let me help your team deliver systems that get it right the first time and build better outcomes for your users.

Experience:

Fractional CSO / Principal Consultant, Systems Structure Ltd.

(May 2017–Present): SSL provides fractional chief security officer services, security architecture and strategy consulting, security compliance certification and policy development assistance, risk and exposure analysis, operational security review, and security engineering culture change support to our clients. We work companies in the software, infrastructure, media, finance, energy, healthcare, and manufacturing industries across the US and Europe. Our engagements are diverse, but teams learning to build or secure infrastructure-as-code, teams facing fundamental security strategy challenges, and teams architecting novel, high-exposure distributed systems have particularly benefited from our work.

Staff Security Architect, Etsy, Inc., New York, NY USA

(May 2016–May 2017): As Etsy's sole security architect, built a principles-oriented security strategy and defined technical interventions to significantly reduce security risk across the company, acted as a technical backstop and mentor for the security team and staff engineering cohort, and provided specific advice and security design for projects including the first internal PKI and kubernetes deployments. Began development of a product security design program and methodology to help cross-functional teams deliver products with better security outcomes for both Etsy members and the company. Worked with a wide variety of internal teams, including legal, compliance, research, and design on security- and privacy-related issues.

Independent Consultant, Remote/International

(October 2012–May 2016): Worked with software teams, news organizations, and NGOs, many working in high-risk contexts with nation-state adversaries, to provide security strategy, risk analysis, architectural and product/system security design guidance, operational security practice and policy reviews, and code review. Worked on messaging systems, payment systems, whistleblowing platforms, data management systems, and a variety of other tools intended for use in this environment. Provided security analysis to a number of open source security projects, including Briar and Mailpile.

Principal Security Engineer, Open Internet Tools Project, Remote

(October, 2012–April, 2014): OpenITP supported developers of counter-censorship, counter-surveillance, and high-risk/targeted endpoint security tools. With OpenITP:

- Provided security and development advice to a large number of software projects
- Structured and built the Peer Review Board (PRB), a project aimed at raising the security standards of humanitarian free software, both across the software development lifecycle and specifically by provisioning commercial audits
- Developed protocols for project and consultancy selection and interaction, disclosure, and audit conflict management, selected and contracted firms, and managed audits

Senior Security Associate, Stach & Liu (now Bishop Fox), Remote

(August, 2010–October 2012): Led engagements with Fortune 500 and government clients:

- Continued development of Trike threat modeling tool, working to extend it to model more complex scenarios balancing multiple perspectives, to handle degradation instead of failure, and to model non-computer resilience scenarios
- Developed the Security Development Lifecycle Consulting practice, including a cohesive vision for how all services integrate across the company
- Co-developed a more effective and faster methodology for designing input validation
- Co-developed tools and methods for development process change, including process change for groups using agile development practices

EXPERIENCE:

Security Consultant, iSEC Partners, Seattle, WA, USA

(November 2008–January 2010): Performed a wide variety of security consulting work for multiple high-profile enterprise clients. While at iSEC Partners:

- Wrote automated security testing tools for web services systems
- Audited code and tested applications and web sites with and without code access
- Wrote an MSDN-published whitepaper and article on ROI and security metrics
- Created training material, guidelines, and standards for both specific customers and general application across multiple languages and development methodologies

Computer Security Engineer, Security Innovation, Inc., Seattle, WA, USA

(January 2006–October 2008): Led threat modeling Center of Excellence and performed consulting work in a variety of security-related roles. While at Security Innovation:

- Audited code and designed system mitigations in complex applications
- Reviewed and (re-)designed architectures and created threat models
- Managed other engineers on a per-project basis
- Wrote a variety of internal fuzzing and security testing tools
- Continued research on, defined offerings and positioning for, and trained other engineers in threat modeling
- Recruited and interviewed technical staff, advised on staffing and professional development, and assisted with sales engineering work

Computer Security Analyst, IOActive, Inc., Seattle, WA, USA

(September 2003–January 2006): As a consultant, audited code, reviewed architectures, and build threat models. At IOActive:

- Designed and developed tools to support security knowledge capture and data analysis
- Managed teams and simultaneous projects with heavy client interaction
- Performed sales engineering, scheduling and project management work
- Performed research in threat modeling to further formal understanding of the security of complex systems, and used the research to guide development workflows

PROJECTS:

Briar/Bramble (2011–Present)

Bramble is a decentralized, transport-agnostic, delay-tolerant communications protocol that ensures confidentiality, integrity, authenticity, and forward secrecy of messages sent via it, and Briar is the user-facing messaging app built on it. Both are designed to be cryptographically rigorous but easy to use, with care given to ensuring Briar's security model matches user expectations. Worked with Michael Rogers on Briar's core protocol, threat model, development process, and user experience design. More information is available at https://briarproject.org.

The Trike Threat Modeling Methodology (2003–Present)

Trike is a unified conceptual framework for analyzing the security of an application ecosystem from a risk management perspective in a reliable, repeatable manner. It and its open source implementation are intended for use by security teams to describe the characteristics of a system from requirements and architecture to implementation and to enable communication among team members and between teams and other stakeholders. It is distinguished from other methodologies by high levels of automation, a defensive perspective, and a high degree of formalism. More information is available at http://octotrike.org.

SKILLS:

Core Skills: Security and engineering strategy, security process and engineering culture change, operational security review, problem solving, research and methodology design and testing, public speaking, client/customer interaction, team management, persuasive and technical writing, sales engineering, project management, and process and workflow design.

Computational Skills: Threat modeling, architectural/whole systems analysis, protocol design and review, white/grey box application security testing and test management, design review, object-oriented design, requirements analysis, and development.

Languages: Python, shell, SQL, HTML, others as needed

EDUCATION:

Case Western Reserve University, Cleveland, OH (1997–2002)

Coursework completed toward a Bachelor of Science in Computer Science with a minor in Artificial Intelligence. Relevant coursework:

- Design theory seminar (grad.)
- User interface design (grad.)
- Software engineering (grad.)
- Systems analysis and organization design (grad.)
- Complex systems modeling and analysis (grad.)
- Object oriented software development (grad.)