# Eleanor Saitta

ella@structures.systems Helsinki/NYC/Remote
https://structures.systems
@dymaxion

## Objective:

I want to continue working with world-class teams to push the cutting edge of security strategy, analysis, and design. I have deep experience in application security, threat modeling, and strategy and particular interests in product security design and usable security for high-risk users. Let me help your team deliver systems that get it right the first time and build better outcomes for your users.

## Experience:

Owner, Systems Structure Ltd.

(May 2017–Present): SSL provides security architecture and strategy consulting, 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, healthcare, and manufacturing industries across the US and Europe, as well as government and non-profit clients. 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 benefitted 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

(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. Provided security analysis to a number of open source security projects like 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 consulting engagements for major Fortune 500 and government clients in multiple countries:

- 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:

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.

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 interaction, team management, persuasive and technical writing, sales engineering, project management, and process and workflow design.

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.)

## Interests:

- Threat modeling and risk analysis
- Service design
- Delay-tolerant networks
- Holistic/outcome-oriented security
- Psycho-social well-being
- Disaster relief
- Embodied experience design
- Physical interface design
- Complex system failures & resilience
- Product security design
- Traffic analysis resistance
- High-risk user protection
- System dynamics
- Human-centric architecture and urbanism
- Ubiquitous computing/IoT
- Sociotechnical systems modeling

## Talks:

Luring Developers with Candy & Other Evil Tricks; KiwiCon X; Wellington, New Zealand; November 2016

Talked about how to ensure a security team is cooperatively integrated into a product organization, what closed-loop security engineering looks like, and product security design.

Ending Online Harassment; The Conference; Malmo, Sweden; August 2015

Spoke on design and engineering strategies to reframe online harassment as a security design issue and effectively end it while preserving user civil rights.

What to Expect When You're Expecting Trouble; Alibis for Interaction; Malmo, Sweden;

Talked about security design from a UX, participation, and design perspective.

Security Keynotes; O'Reilly Velocity; Amsterdam, The Netherlands, and Santa Clara, CA; October 2015 and June 2016

Talked about security design and its place in the software security lifecycle.

Security Design and High-Risk Users; Hack in the Box GSEC; Singapore; October 2015 and Hack.Lu, Luxembourg; October 2015

Talked about how lessons from high-risk users can inform general-purpose application security.

Threat Modeling and Security Test Planning, HOPE, NYC; July 2014

Introductory talk on threat modeling and the security testing process with special reference to high-risk user needs.

Tegenlicht, VPro; Netherlands; February 2014

Broadcast appearance on surveillance and economics on the largest Dutch public affairs weekly.

No Neutral Ground in a Burning World; 30c3; Hamburg, Germany; December 2013

Spoke with Quinn Norton on how technology changes relationships between people and with authority across centuries, and on the social and emotional impacts of the Internet.

Ethics and Power in the Long War; OHM; Amsterdam, Netherlands; August, 2013

Spoke on the structure and economics of state surveillance and the technical community's responsibilities and opportunities for responding to it.

Yale Law School Protecting Journalism Conference; New Haven, USA; November 2012

Spoke on a panel on trade-offs and synergies between security and usability for high-risk users.

The Fight for the Internet; The Guardian; Online Video Debate; October 2012

Appeared in a Guardian video debate on the future of Internet governance.

Hands on Threat Modeling with Trike v1: ToorCon 7; San Diego, USA; August 2005

The first public talk on Trike, presented with Brenda Larcom, the other half of the Trike team.

## Publications:

Patreon Essay Series; September 2015–Present

My on-and-off on-going series of writing on security- and systems-related issues, averaging about 12,000 words a month. The first piece, "Please Stop Writing Secure Messaging Tools" was read by over 40,000 people. See https://dymaxion.org/essays/

Real World Use Cases for High-Risk Users; May 2014

A short catalog presenting some use cases for high-risk users to shift the dialog in the security tools community toward tools for individuals with fewer resources dealing with small adversaries, since adopted and expanded by Simply Secure and others.

The Key to Ending Mass Surveillance? Math.; The Nation; June 2015

An essay arguing for encryption as our only effective way to contain bulk foreign intelligence surveillance.

Microsoft SDL: Return On Investment: MSDN, September 2009

This whitepaper and the accompanying MSDN SDL blog post describe how to track and understand the impact of security investments, and provide guidelines for determining resource allocations. Note: credited to another iSEC Partners employee for PR contact reasons.

Trike v1 Methodology Document, July 2005

The formal methodology document for the Trike threat modeling methodology; now superseded by further (currently unpublished) research.

## Workshops:

RightsCon International Criminal Court Digital Forensics Workshop and Access Prize Judging; San Francisco, USA; March 2014

Acted as a judge for the 2014 Access Prize for endpoint security, awarded to the Tails Linux project. Also advised the International Criminal Court on tools and techniques for handling digital evidence of crimes against humanity and evidence security.

Open Humanitarian Initiative Code Sprint; Birmingham, UK; September 2013

Worked with the Taarifa project team to explore the combination of decentralized delay-tolerant networking and open workflow management systems in civic management, development aid, and complex and natural disaster scenarios.

Brussels Meeting on Surveillance; Brussels, Belgium; October 2012

Meeting of a number of Internet policy, civil society, and security actors with the intent of taking a proactive stance against police surveillance. Resulted in the creation of the International Principles on the Application of Human Rights to Communications Surveillance.

Joint Interagency Field Experimentation: Research & Experimentation for Local & International Emergency First Responders (JIFX RELIEF/Camp Roberts); Paso Robles, USA; August 2012 and February 2013

Camp Roberts is an ongoing HA/DR early-stage (TL 4/5) field prototype integration trial environment. Participated as an observer and invited security expert.

Circumvention Tech Summits; Rio de Janiero, Brazil, Tunis, Tunisia, Hong Kong, and Berlin, Germany; June, 2012, November 2012, April 2013, and September, 2013

The OpenITP Circumvention Tech Summit series brings together engineers, trainers, experts in security and usability, and field actors to network, examine the challenges currently at hand, and work together to find opportunities to collaborate. Participated as both a security expert, a representative of the Briar and Trike projects, and a member of the organizing team.