David Stainton

E-mail: dstainton415@gmail.com
Work Portfolio: https://sphinx.rs/
Github profile: https://github.com/david415
Twitter profile: https://twitter.com/david415
LinkedIn profile: https://www.linkedin.com/in/david-stainton

Software Developer

• **Rust**	★★★☆☆	• **Python**	★★★★☆
• **Golang**	★★★★★	• **C**	★★☆☆☆

Career Summary

I have over twenty years experience as a software developer. For the past six years, I have worked as a security specialist focusing on cryptographic protocols, anonymous communication networks and network forensics.

The Edward Snowden document leaks inspired me to write a TCP protocol analyzer for detecting injection attacks. During the course of this 'Honeybadger' project, I created the most comprehensive categorization of TCP injection attacks. Please see my work portfolio website for more information about Honeybadger.

While attending a 2017 Tor developer meeting in Amsterdam, I began to work on the Panoramix project: to design and build the Katzenpost decryption mix network. During this time, I oversaw a collaborative effort to write design specifications and software. I also led the acquisition of funding from additional grant programs.

Currently, I design and write commercial cryptography software for SpiderOak Inc. At SpiderOak, I also coordinate a cryptography paper reading club to encourage my co-workers to cultivate familiarity with the contemporary discourse around cryptography.

Researcher Collaborations

- George Danezis, University College London, UK, collaborated within Panoramix H2020-653497
- Claudia Diaz, KU Leuven, Leuven, Belgium, collaborated within Panoramix H2020-653497
- Research visit to KU Leuven with Claudia Diaz and Tariq Elahi on February 5th 2018, Leuven, Belgium, collaborated within Panoramix H2020-653497
- Daira Hopwood, Least Authority, Open Technology Fund, US government grant to work on the Tahoe-LAFS "magic-folder" system.

Security Systems Design

- H2020 EU project Panoramix (Privacy and Accountability in Networks via Optimized Randomized Mix-nets)
  Co-designed the Katzenpost Mix Network as part of the Panoramix academic grant project with collaborators: George Danezis, Claudia Diaz, Ania Piotrowska and Yawning Angel. https://panoramix-project.eu/
  https://github.com/katzenpost/docs/tree/master/specs
- Co-designed the Tahoe-LAFS "magic-folder" with collaborators: Daira Hopwood. Magic-folders is an extension of Tahoe-LAFS that automatically synchronizes filesystem changes within a designated directory hierarchy. This is done with end-to-end encryption so that confidentiality of files is maintained. Design specification documents available here: https://github.com/tahoe-lafs/tahoe-lafs/tree/master/docs/proposed/magic-folder

Open Source Contributions

- My Github Profile: https://github.com/david415
- My Rust, Golang and Python software contributions, see here:
  https://sphinx.rs/projects/

Public Speaking

- I have plenty of public speaking experience giving talks at Security, Privacy and Crypto Currency related events and conferences. For details see here:
  https://sphinx.rs/publicspeaking/
- My most memorable public talk was held at Eindhoven University in Netherlands at the Security in Times of Surveillance 2019. It was a great honor to speak their, however unfortunately the video recording has not yet been made publicly available.
  https://www.win.tue.nl/eipsi/surveillance.html

Formal Education

- General Education Diploma

Professional Experience

SpiderOak Inc., remote work, Senior Software Developer July 2020 – Present

- made many code contributions
- wrote design specification documents
- collaborated in the design of custom cryptographic protocols
- wrote cryptography software
- made use of various technologies such as: **Golang, Docker, AWS Key Management Service, MinIO, sqlite, TLS OCSP**.

Katzenpost open source project, remote work, Software Developer Jan 2019 – Present

- After the Panoramix project officially ended I led the acquisition of further funding from both Samsung Next and NLNet grant programs.
  - https://nlnet.nl/project/katzenpost
  - https://opencollective.com/the-katzenpost-software-project

  Some of the technologies used on this project: **Golang, Boltdb, Prometheus, Docker, Travis CI, Gitlab CI, and the Noise cryptographic protocol framework**.

CCT gGmbH, remote work, Software Developer Apr 2017 – Jan 2019

- Collaborated in the design and implementation of the Katzenpost mix network for the H2020 EU project Panoramix (Privacy and Accountability in Networks via Optimized Randomized Mix-nets) https://panoramix-project.eu/.
- Katzenpost source code: https://github.com/katzenpost
- I was a speaker at various security and privacy conferences where I introduced our software project and gave a brief overview of mix networks.
- Contributed many Katzenpost software components including client and server networking, custom cryptographic protocols etc.

Least Authority, remote work, Software Developer Dec 2013 – Apr 2017

- At Least Authority I made many Python code contributions to the Tahoe-LAFS cryptographic storage open source software project. https://tahoe-lafs.org/trac/tahoe-lafs
- I also worked with the Least Authority AWS setup which included usage of EC2 and S3.

The Beginning Of My Career

In the beginning of my career from 1998 to February of 2013 I worked in the San Francisco bay area and in Germany primarily as an Network Tools Developer and Operations Engineer at the following companies: Zenmate, Addvocate, Causes, Scribd, Spinn3r, Snapjot, Snapfish, Barracuda Networks, DataDomain, Northpoint Communications and, CRL Network Services.