Christopher Patton

219 MAE
CISE
University of Florida

Email: cjpatton@{ufl,ucdavis}.edu
Homepage: cjpatton.sdf.org

I am a Ph.D student in cryptography at the University of Florida working with Tom Shrimpton.

Education

M.S. Computer Science. University of California, Davis - 2015.

B.A.S. Computer Science and German. University of California, Davis - 2013.
Study abroad - Free University, Berlin, Germany - 2010/2011 Academic year.

Academic interests

My research focus is cryptography with an emphasis on practice oriented, provable security. I've studied a modest, but growing variety of problems in this tradition, including authenticated encryption, anonymous communication, and hedged public-key encryption. I'm interested in developing crypto-for-privacy[1] as a discipline and providing tools that enable the tech industry to build privacy into their systems from the start. Past and pending interests include computational theory, complexity theory, algebra, coding theory, and programming language design and semantics.

Projects

Chrome protector (Internship at Google-Montréal, summer 2016). This summer I worked on the Chrome protector team, who's task is to defend users from malware and other unwanted software. The main thrust of my work was to study ways in which malicious code gets injected into Chrome. My project improves the team's ability to detect malware campaigns in the wild. I also explored the use of the Riposte cryptosystem[2] for anonymously collecting reports of potential security incidents.

Cloud security (Internship at Google-Kirkland, summer 2015). I worked on the cloud security team at Google. CloudProxy is an open source project that cryptographically binds the identity of a service (that is, its public key) to the code that executes it, as well as the environment in which it executes. My project involved bringing this platform to bear on production servers at Google. I also worked on the open source codebase and implemented an application for the platform. See `github.com/jlmucb/cloudproxy` (navigate to go/apps/mixnet/README.md) for a brief description of the CloudProxy and the application.

QRAAT (2013—2015). The QRAAT ("Quail Ridge Automated Animal Tracking") system is designed to provide ecologists and animal biologists with high resolution animal tracking data in real-time. It is comprised of a network of radio receivers deployed across the Quail Ridge Nature Reserve in Napa Valley, California, and uses radio telemetry to track species ranging in size from small field mice to large foxes. The goal is to deliver a complete hardware and software platform that can be deployed to other locations

[1] See Phil Rogaway's paper "The moral character of cryptographic work" for the etymology of this term.
[2] See Henry Corrigan-Gibbs' paper "Riposte: an anonymous messaging system handling millions of users".

and studies. My masters thesis reviews the state of animal tracking in the literature and provides a detailed analysis of our own methodology. Visit the project site at `qraat.ucdavis.edu`.

Qurinet (2012—2013). Qurinet is an experimental, wireless, solar-powered mesh network that provides the network infrastructure for the QRAAT project, as well as a myriad of monitoring equipment. My responsibilities included network administration and site reliability. I also assisted in experiments on Qurinet for the networking lab at UC Davis.

YAMZ metadictionary (Internship at DataONE, summer 2013). YAMZ (formally SeaIce) is a crowd-sourced dictionary that provides a forum for defining a set of common terms for annotating datasets. Modelled loosely on StackOverflow, it uses a reputation-based voting system to drive the classification of terms as useful or not. I developed the prototype, which is still live at `yamz.net`. I am no longer the maintainer.

Skills and experience

Software engineering. My favorite languages are C/C++, Go, and Python. I have experience writing bash, Objective C, Standard ML, Perl, and Java. I am very familiar with GNU/Linux and version control with git. I have experience with: database systems MySQL and PostreSQL and their Python interfaces (QRAAT and YAMZ), web development with the Django framework for Python (QRAAT), build systems cmake and the GNU autotools, the madness of SWIG, source documentation with doxygen and Python-Sphinx, and image processing in OpenCV.

Network administration. Low-level management of network resources. Configuration of link and routing layer protocols, in particular 802.11/n and OLSR respectively; experience with firewall management with iptables, and familiarity with command line diagnostic tools (Qurinet). Management of a web service with Apache, MySQL, and Python-Django (QRAAT).

Embedded systems. Installation and customization of headless, power-limited systems with the GNU/Linux distribution OpenWRT. This includes customization of the Linux kernel and cross-compiling software for the target environment. (QRAAT and Qurinet.)

Teaching. I've been a teaching assistant for undergraduate courses in discrete mathematics (for computer science students) and cryptography. I lead discussions, held office hours, graded exams and homework, and even had a couple opportunities to give the lecture.

References

Cait Phillips, Chrome protector, software engineer at Google — `caitkp@google.com`

Tom Roeder, Cloud security, software engineer at Google — `tmroeder@google.com`

Marcel Losekoot, project manager for QRAAT — `mlosekoot@ucdavis.edu`

Last updated: September 16, 2016