Caleb Madrigal

- caleb.madrigal@gmail.com
- 414-215-0003
- Milwaukee, WI
- http://calebmadrigal.com
- https://github.com/calebmadrigal
- https://twitter.com/caleb_madrigal
- https://www.linkedin.com/in/calebmadrigal

Description

I like programming, hacking, and mathing! Since high school, I've been into network programming, cryptography, and security stuff, and I consider that my forte. In my free time, you'll often find me playing with things like Software-Defined Radio, making or hacking IoT devices, or doing with mathy things. On the math-side of stuff, I'm most interested in using math to see things that are otherwise difficult - pulling the signal out of the noise.

Though I've had experience with fluffy languages like Javascript and .NET (don't count that against me! It's a symptom of living in the midwest!), I can write some tight C code, though if I have my druthers, I usually write it in Python.

On a personal note, I try to be humble and kind to everyone. I think I'm a pretty likable person (or else, I just can't read people at all :)).

Skills

- Expert understanding of Network and IoT security, as well as other security-related topics like Cryptography
- Strong algorithms and mathematics knowledge
- Strong communicator
- Expert functional programmer (and of course, I can do OOP too)
- Good at data analytics and visualization (IPython Notebook/Jupyter/NumPy/SciPy/Matplotlib, d3)
- Good at front-end design (Responsive Design, SVG, Photoshop)
- Team leadership experience

Technologies and Tools

- Languages/Platforms:
  - Python (ctypes, Jupyter/NumPy/SciPy/Matplotlib/Pandas, ctypes, asyncio, ZeroMQ, Flask, Django, nose, unittest)
  - Javascript (Node.js, React.js, AngularJS, d3.js, Express.js, Underscore.js, Lodash.js, Async.js, jQuery, q, mocha, jasmine)
  - C (gcc, sockets, linux, makefile)
  - Web (HTML5, CSS3, Bootstrap/Responsive Design, Javascript - see above)
  - Objective-C (iOS, Cocoa)
  - C# .NET (ASP.NET, Web API, MVC4, NHibernate, Spring.NET)
  - Clojure, Scheme, Lisp
  - Java EE (GWT, JSF, Spring, Hibernate)
- Security tools: Scapy (packet crafting), Yara, HopperApp (a poor man's IDA Pro), RedLine (a

Mandiant tool), various FireEye offerings, the obvious things like nmap
- Databases: PostgreSQL, Redis, MSSQL, MySQL, MongoDB, IBM DB2, Sqlite
- Software packaging: Linux package creation (rpm and deb) and Mac package creation
- Other Tools: Docker, Vagrant, VirtualBox, VMWare Fusion/Workstation, Team City, Visual Studio, IntelliJ, PyCharm, WebStorm, Photoshop, iDraw
- Linux Server configuration: iptables, Nginx, Apache, SysV/Systemd/Upstart, sendmail, cron
- Version Control: Git, SVN

Experience

Mandiant/FireEye

Senior Software Engineer, *April 2015 - Present*

- *Technologies:* Python, C, ctypes, redis, Node.js, Mac, Linux, Windows
- Wrote host-side (agent) and server-side software for Incident Response investigations.
- Software automates various Incident Response scans, and provides consultants with powerful investigative capabilities.
- Here are a few of my personal accomplishments on the project:
  - I spearheaded the expansion of the our agent from Windows to both the Mac and Linux platforms.
  - I designed and implemented the code signing system for our job system.
  - I designed and implemented various mechanisms for improving connectivity robustness, such as methods for getting through Deep-Packet Inspecting Firewalls.
  - I made many significate performance improvements to the system.
  - I came up with innovative networking solutions to strict customer requirements, and communicated those solutions to high-value customers.

SpiderLogic

Software Consultant, *March 2011 - April 2015*

Client: Wisconsin Lawyers Mutual Insurance Company, 2013-2015

- *Technologies:* Node.js, Express.js, AngularJS, MongoDB, Java, SOAP, Oracle, Linux
- Lead a small team to create a web portal for a legacy enterprise Java policy administration system. This allows clients to pay premiums and renew their policies via the web (previously a paper transaction).
- The front-end was implemented as a Single-Page App (with AngularJS, and Bootstrap).
- Backing the front-end was a "smart proxy" (written in Node.js, Express.js, and MongoDB) which presented the front-end with a nice RESTful API, and which abstracted away the dirty details of making all kinds of complex SOAP calls to the legacy Java system.
- I built the smart proxy into the design not only to make the front-end simpler, but also because the client was considering moving away from their legacy Java policy administration system, and the smart proxy would allow them to more easily replace it with minimal impact to the web portal codebase.
- Wrote integration tests in Python which validated that the legacy Java service layer was behaving as expected.

Client: Hewins Financial, 2013-2015

- *Technologies:* Java EE, Google Web Toolkit, MySQL, Linux, Python, ZeroMQ
- Created a web app which enables financial advisors to rapidly model their clients' financial outlook and walk them through various financial scenarios.

- Created an offline version of the app by wrapping the server software in a Virtual Machine.
- For the offline version of the app, I wrote a protection layer in Python (web app and daemon) which required users to log in, and periodically would check with the server that they still are authorized to use the app. If a user was no longer authorized (or the protection layer was unable to contact the validation server in a given time period), then the protection layer would disable the app. This protection layer used ZeroMQ to communicate between its subprocesses.

Client: MyHealthDirect, 2012-2013

- *Technologies:* C# .NET, ASP MVC4 .NET, Spring, NHibernate, MS SQL, Objective-C
- Wrote Medical scheduling web app and iPad app.
- Use Python to write an ETL tool to transform client-provided data files into a format our database could handle. It allowed us to write mapping files which specified how to map columns and transform data.
- Helped maintain large enterprise API and web app.

Client: Wipfli (Internal Development), 2012

- *Technologies:* Objective-C
- Wrote insurance risk analysis iPad app which allows risk prevention field workers to survey insured properties, take pictures and record notes of potential liabilities, and submit their reports to the back office.

Client: SoZo Group, Wipfli (Joint Venture), 2012

- *Technologies:* Javascript, HTML5, CSS3, Joomla CMS, PHP, Linux
- Created web informational portal to provide help to Chinese companies looking to move operations to the US.

Client: ScenarioNow, 2011-2012

- *Technologies:* Java EE, Google Web Toolkit, MySQL, Linux
- Wrote financial modeling software for financial advisors.

Client: Church Mutual Insurance Company, 2011

- *Technologies:* Java EE, Spring, Hibernate, JSF, IBM DB2
- Wrote Java EE application to manage actuarial statistics for Insurance Rating Software.

Astronautics Corporation of America

Software Engineer, *June 2008 - March 2011*

- Wrote software in the C programming language for the Airbus A400M Network Server System (NSS).
- Developed several APIs based on requirements which I gathered from multiple teams.
- Developed company-wide Python coding standard and gave training presentations on Python.
- Wrote a hardware emulator in Python for use in our labs. It communicated via RS-232, and allowed us to mock out this particular hardware device. It also allowed us to set various states on this hardware device to ensure other systems behaved correctly.
- Wrote various integration tests in Python.
- Wrote Software design documents which used UML diagrams to communicate software module design and interactions.
- Authored the Software Requirements Document for one of the components for the NSS in IBM

Rational Doors (requirements tracking software).
- Wrote Test Cases, Test Procedures, and Test Applications (in C and Python) to verify requirements.
- Followed DO-178B for process flow, requirements, testing, implementation, etc.

Hitcents

Software Engineer, *August 2006 - May 2008*

- Developing an Enterprise Resource Planning (ERP) system.
- Desktop front-end to ERP in C# .NET/XAML/WPF
- Integrated Microsoft Office with ERP system.
- Used Python to write socket-level communication system for both the server-side and front-end of ERP to provide push notifications to our desktop client (as well as receive messages pushed to the server from the client).
- Wrote web software for ERP system using Perl, Javascript, CSS, and HTML.
- Developed access control software that uses Radio Frequency Identification (RFID).
- Certified RFID specialist at Hitcents.

Teksouth

Programming Summer Intern, *May 2005 - August 2005*

- Wrote a program that controlled the magnetic front door lock, using MS Outlook calendar as a front end for scheduling.

Side Projects/Research

Tracker Jacker

- https://github.com/calebmadrigal/tracker-jacker
- Monitors raw 802.11 frames to do things like:
  - Track a person by their phone's MAC
  - Detect when motion-sensing security by looking for a threshold of traffic (indicating video upload)

Truthy Graph

- Live app: https://truthygraph.github.io/
- Simple graphing app which graphys "truthiness" of an equation (a gradient of how close to equal the two sides of the equation are).

SDR Radio hacking scripts

- https://github.com/calebmadrigal/radio-hacking-scripts
- Various scripts for capturing and signals with SDR.

Network hacking scripts

- https://github.com/calebmadrigal/network-hacking-scripts
- Various scripts for performing surveilling and attacking LANs.

Vanguard investment analysis

- https://github.com/calebmadrigal/investment-analysis
- Analyzed historical returns of Vanguard mutual funds to help me understand things like how volatility and expected return are correlated, and to help me find the best mutual funds to invest in.

Home Security System

- http://calebmadrigal.com/raspberry-pi-home-security-system/
- For fun and security, I built a home security and automation system.
- Hardware: RaspberryPi, hacked remote controlled outlet set, hacked magnetic sensor
- Software: Python, Flask, jQuery Mobile, ZeroMQ

Other Side projects

- See http://calebmadrigal.com and http://github.com/calebmadrigal for my most recent side projects.

Speaking

Cyphercon 2017

Topic: Tracking/monitoring WiFi devices without being connected to any network

- Presentation related software: https://github.com/calebmadrigal/tracker-jacker

DC414 Meetup (December 2016)

Topic: Intercepting, modifying, and generating wireless signals with SDR

- Related code:
  - https://github.com/calebmadrigal/radio-hacking-scripts/blob/master/radio_signal_generation.ipynb
  - https://github.com/calebmadrigal/radio-hacking-scripts/blob/master/generate_digital_signal.py

Cyphercon 2016

Topic: 2 mini-talks: Hypervault and Tunneling

- Hypervault app presented on: https://hypervault.github.io/
- Tunneling topic notes: http://calebmadrigal.com/dns-tunneling-with-iodine/

O'Reilly Open Source Convention (OSCON) 2013

Topic: Sound Analysis with the Fourier Transform and Python

- Presentation Notes/Code: https://github.com/calebmadrigal/FourierTalkOSCON

Milwaukee Barcamp 2011

Topic: Using Transparent HTTP Proxies for Live Web Traffic Manipulation

- Code used:

https://github.com/calebmadrigal/PythonScripts/blob/master/networking/httpproxyserver.py

Education

Bachlor's in Computer Science - Western Kentucky University

- GPA: 3.80 on a 4.0 scale (Graduated May 2008)
- ACM President of WKU local chapter (2007-2008)
- Future Leader Award in Computer Science (2008)
- President's Scholar at WKU (2007-2008)

Other Classes

- DevelopMentor Modern ASP.NET (2014)
- Coursera Machine Learning class with Angrew Ng - https://www.coursera.org/course/ml (2013)
- Udacity Artificial Intelligence for Robotics (2012)
- Stanford Artificial Intelligence class with Sebastian Thurn and Peter Norvig (2011)