

# Caleb Madrigal

- caleb.madrigal@gmail.com
- 414-215-0003
- <https://madconsulting.ai/>
- <https://calebmadrigal.com>
- <https://github.com/calebmadrigal>
- <https://www.linkedin.com/in/calebmadrigal>
- [https://twitter.com/caleb\\_madrigal](https://twitter.com/caleb_madrigal)

## Description

I specialize in Cybersecurity, Machine Learning, and building software.

## Experience

### Mad Consulting

**Co-Founder, *January 2020 - Present***

- *Technologies:* Python, React, Tensorflow, Keras, Jupyter, Spark
- Various projects for clients.

### Mandiant/FireEye

**Senior Software Engineer, *April 2015 - January 2020***

- *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 significant 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).

**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.

**Client: MyHealthDirect, 2012-2013**

- *Technologies:* C# .NET, ASP MVC4 .NET, Spring, NHibernate, MS SQL, Objective-C
- Wrote Medical scheduling web app and iPad 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).

## **Hitcents**

**Software Engineer, August 2006 - May 2008**

- Developing an Enterprise Resource Planning (ERP) system.
- Desktop front-end to ERP in C# .NET/XAML/WPF
- 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).
- Developed access control software that uses Radio Frequency Identification (RFID).

## 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

### <https://gods.art>

- I paint with math at <https://gods.art/>

### Tracker Jacker

- <https://github.com/calebmadrigal/trackerjacker>
- 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

### DEF CON 2017

- Topic: Controlling IoT devices with crafted radio signals
- Presentation: <https://www.youtube.com/watch?v=qhuhJ9Oe9vA>

### THOTCON 2018

- Topic: Inferring wireless camera motion detection without being connected and other 802.11 IoT hacks
- Presentation related software: <https://github.com/calebmadrigal/trackerjacker>

### DEEPSEC 2018 (in Vienna)

- Topic: Inferring wireless camera motion detection without being connected and other 802.11 IoT hacks
- Presentation related software: <https://github.com/calebmadrigal/trackerjacker>

### THOTCON 2017

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

### Cyphercon 2017

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

### Cyphercon 2017

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

### 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) 2015

- Topic: Building a modern UI for programmers
- How to quickly build a descent UI if you're not a designer

### 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/calebmadrighal/PythonScripts/blob/master/networking/httpproxyserver.py>

## **Education**

- Life
- Bachelor's degree in Computer Science - Western Kentucky University