Greg Cusack

Ph.D. Student and Graduate Research Assistant

Aiming to make large-scale, networked applications and the
underlying infrastructure efficient and simple to deploy,
manage, monitor, and secure in multi-tenant environments

805-698-6998

gregorycusack@gmail.com

github.com/gregcusack

linkedin.com/in/gregorycusack

gregcusack.github.io

Boulder, Colorado

Education

University of Colorado, Boulder CO **Fall 2017-Present**
- Ph.D. student in Computer Engineering, Computer Networks and Security (GPA: 3.85)
- Graduate Research Assistant in Network and Security Research (NSR) Lab

University of California, Los Angeles CA **Fall 2016-Spring 2017**
- Master of Science in Electrical Engineering, Embedded Systems (Not completed)
- GPA: 3.91 (Left UCLA 2 classes early to pursue Ph.D. at CU Boulder)

Santa Clara University, Santa Clara CA **Received: June 2016**
- Bachelors of Science in Computer Science and Engineering and in Electrical Engineering
- *magna cum laude* (GPA 3.76), Tau Beta Pi, Upsilon Pi Epsilon, Dean's List
- Researched under Dr. Shoba Krishnan designing a low-cost, mobile device to detect arsenic in water

Research

Elastic Containers | *Project Lead* **Spring 2019 - Present**
- Lead a four person team (3 Ph.D. students and 1 Masters student) in designing and building a container management solution for large scale cloud applications
- <u>Goal</u>: To improve resource utilization and application throughput, while also abstracting away per-container resource provisioning and management for large microservice applications
- <u>Method</u>: Instead of enforcing per-container limits on compute resources (as is the norm and only way), we set *per-application* limits on compute resources (CPU and memory). When an application is deployed, the underlying containers consume computing resources as needed to meet demand while cumulatively remaining at or below the per-application resource limit.
- <u>How</u>: Resources are allocated to each underlying container by a global manager in an "as needed" fashion that takes into account current CPU loads, memory demands, and the remaining compute resources available to the application.
- <u>Responsibilities</u>: Project task management, modifying the Linux kernel and its CFS scheduler, and building a centralized manager to monitor the distributed container resources
- **Result: poster to appear at ACM CoNEXT 2019 Posters**

Cloud-Scale Packet-Level Network Analytics in Software **Fall 2017 - Present**
- <u>Goal</u>: Design a general and flexible, packet-level, network analytics system on top of P4 switches
- <u>Method</u>: Optimize at the network analytics platform level rather than at a per-application level
- <u>How</u>: Eliminate choke points. Push system tasks into hardware and exploit workload characteristics to eliminate cross-core communication and high data structure overheads.
- <u>Responsibilities</u>: Developed a machine learning-based ransomware detector, a network intrusion detection system, and network denial of service identification systems that run on top of the analytics platform. Built the back-end of the analytics platform for packet-level data aggregation and visualization.
- **Result: full length paper currently in submission**
- **Result: poster (won best technical poster) and paper published at NDSS 2018 and SDN/NFV Sec'18, respectively**

Adversarial Examples for Network Security   Summer 2018 – Fall 2019
• Goal: Analyze how state-of-the-art neural network-based network intrusion detection systems (NIDSs) are vulnerable to adversarial examples (attacks).
• Method: Learn from adversarial examples in the image domain and craft adversarial examples for neural network-based NIDSs in the highly-constrained network domain.
• How: Define the network domain-specific legitimate transformations an adversary can apply to his or her malicious network traffic such that the attack appears benign. Build adversarial attacks using said transformations.
• Responsibilities: Defined legitimate network transformations for various attacks. Built an automation tool to manipulate packets to match target adversarial example network shape.
• **Result: paper published at AISec'18**
• **Result: paper to appear at ACM CoNEXT Workshop - Big-DAMA 2019**

Reconfigurable Secure Hardware   Fall 2017-Winter 2018
• Goal: Design flexible, reconfigurable secure hardware that allows users to control secure hardware features and updates, while also allowing them to choose their root-of-trust.
• Method: Use FPGAs to self-provision keys that are never externally exposed. Implement a secure update mechanism whose policies are defined by the secure hardware application.
• Responsibilities: Built a password manager on top of SGX and our FPGA-based secure hardware to analyze performance differences.
• **Result: paper published at FPGA 2019**

Experience
(Industry)

TransMarket Group | *Software Engineer Intern*   Summer 2017
Chicago, IL
• Designed an automated testing framework in Python, C++, Robot Framework for exchanges around the world to manage catastrophic risk
• Dramatically improved developers ability to identify bugs quickly and effectively in a million-plus LOC trading platform

Texas Instruments | *Applications Engineering Intern*   Summer 2015
Santa Clara, CA
• Developed software to streamline automation for new silicon validation and benchmarking

Honors

Computer Engineering Outstanding Senior Award | *SCU*   June 2016
• "Presented to a senior by the faculty of the Computer Engineering Department based on academic standing, esprit de corps, and contribution to the department, school, and community."

Alpha Sigma Nu | *Jesuit Honor Society*   Spring 2015
• Accepts students in top 15% of junior/senior class who distinguish themselves in scholarship and service to others. It is among the highest honors bestowed at a Jesuit Institution

Skills & Knowledge

C/C++ | Python | Computer Network Systems | Network Security | Linux CFS Scheduler |
Kubernetes | Docker | Ansible | Serverless | Blockchain | Leadership| Problem Solving |
Time Management | Explaining complex information and problems to both engineers and non-engineers

Interests

Linux Kernel | Computer Network Systems | Network Security | Venture Capital | Road Biking | Trail Running | Swimming | Rugby | Improv

Classes	<u>CU</u>	<u>UCLA</u>
	DevOps in the Cloud	Adv. Computer Networks
	Adv. Computer/Network Systems Security	Networked Embedded Systems
	Censorship Circumvention	Software Engineering
	Security and Ethical Hacking	Entrepreneurship and Venture Initiation[1]
	Developing the Industrial IoT	
	Natural Language Processing	
	Venture Capital & Private[2]	

Other   For a research statement, visit my website: gregcusack.github.io/

Publications

(poster) Efficient Microservices with Elastic Containers
Greg Cusack, Maziyar Nazari, Sepideh Goodarzy, Prerit Oberai, Eric Rozner, Eric Keller, Richard Han
ACM CoNEXT (CoNEXT '19 Posters). December, 2019

Towards the Evaluation of NIDSs in Adversarial Settings
Mohammad J. Hashemi, Greg Cusack, Eric Keller
3rd ACM CoNEXT Workshop on Big DAta, Machine Learning and Artificial Intelligence for Data Communication Networks (Big-DAMA 2019). December, 2019

Toccoa: Cloud-Scale Packet-Level Network Analytics in Software
(In Submission)
Oliver Michel, John Sonchack, Greg Cusack, Maziyar Nazari, Eric Keller, Jonathan M. Smith

Breaking the Trust Dependence on Third Party Processes for Reconfigurable Secure Hardware
Michael Coughlin, Greg Cusack, Jack Wampler, Eric Keller, Eric Wustrow
27th ACM/SIGDA International Symposium on Field-Programmable Gate Arrays. February, 2019

Stochastic Substitute Training: A Gray-box Approach to Craft Adversarial Examples Against Gradient Obfuscation Defenses
Mohammad J. Hashemi, Greg Cusack, Eric Keller
ACM Workshop on Artificial Intelligence and Security (AISec) with the 25th ACM Conference on Computer and Communications Security (CCS). October, 2018.

Machine Learning-Based Detection of Ransomware Using SDN
Greg Cusack, Oliver Michel, Eric Keller.
ACM International Workshop on Security in Software Defined Networks & Network Function Virtualization (SDN-NFV Sec). March, 2018

(poster) Machine Learning-Based Fingerprinting of Network Traffic Using Programmable Forwarding Engines
Greg Cusack, Oliver Michel, Eric Keller
Network and Distributed System Security Symposium (NDSS). February, 2018. (won best technical poster)

---

[1] UCLA Anderson School of Management
[2] CU Leeds School of Business

(poster) Time Analysis of the Feasibility of Vehicular Blockchains

Joshua Joy, Greg Cusack, Mario Gerla