Tillson T. Galloway

+1(843) 801-2005 ◇ Atlanta, GA
tillson@gatech.edu ◇ linkedin.com/in/tillson ◇ tillsongalloway.com

RESEARCH INTERESTS

My research focuses on understanding and addressing sophisticated threats against computer networks and systems. I propose and analyze attacks against network security defenses, including intrusion detection systems and state-of-the-art machine learning models, then help make them more robust to the attacks. I am also interested in bridging this academic work with deployable, operational software.

EDUCATION

Doctor of Philosophy in Electrical and Computer Engineering Aug 2022 -
Georgia Institute of Technology
Advisor: Manos Antonakakis

Bachelors of Science in Computer Science June 2018 - May 2022
Georgia Institute of Technology GPA 3.79

PUBLICATIONS

- **Galloway, T.**, Karakolios, K., Ma, Z., Perdisci, R., Keromytis, A., Antonakakis, M., "Practical Attacks Against DNS Reputation Systems"
  Currently under review, pre-print available upon request

RESEARCH AND WORK EXPERIENCE

Georgia Institute of Technology Aug 2022 - Present
Graduate Research Assistant with Manos Antonakakis *Atlanta, GA*
I built an operational, state-of-the-art DNS-based reputation system using terabyte-scale datasets (passive recursive DNS logs, WHOIS data, BGP announcements, etc.), then ran them on a 120TB+ RAM and 8000 CPU Spark cluster. I proposed attacks that allow an attacker to evade DNS reputation models with 100% accuracy for under $25.

Corelight, Inc. June 2022 - Aug 2022
Research Intern *Remote*
I deployed Zeek scripts that detected domain controller activity and lateral movement techniques in large-scale Windows environments. I implemented a signature-based detection for a recent Windows Server NTLM exploit (deployed in the product and open-sourced on GitHub with an accompanying blog post). I also experimented with deep learning-based anomaly detection for NTLM/Kerberos/SMB Zeek logs using LSTMs in PyTorch.

Network Security Startup May 2021 - Aug 2021
Research Intern *Atlanta, GA*

Georgia Institute of Technology Oct 2018 - May 2022
Undergraduate Research Assistant with Manos Antonakakis *Atlanta, GA*
I worked on some of the distributed systems around the lab. For example, I made optimizations resulting in a 50% runtime decrease for an open-source pcap to DNS query parser written in Go. I also created a React web panel to track the lag between data transformation/loading tasks in Apache Spark and the head of an Apache Kafka stream containing DNS resolution information from clients around the world.

Facebook, Inc. Aug 2020 - Nov 2020
Software Engineering Intern *Remote*
I created a system to link legal policy decisions with code paths using inline code annotations. The system ensured that code complied with relevant, up-to-date legal policies and protected user privacy by determining which user data could be released to government entities in response to data requests or warrants.

New Relic, Inc. May 2019 - Aug 2019
Application Security Engineering Intern *Portland, OR*
I built a script that scans GitHub for secrets, saving the company over $10,000 in potential bug bounty payouts. I also wrote scripts to reduce false-positive rates of our Snyk application vulnerability scanners by 40%.

PROJECTS

- **Underground Marketplaces.** Jan 2023 - Present
  I collected over 20,000 compromised domains and 10,000 compromised IP addresses being sold on a popular underground marketplace and am studying the economics of the marketplace, the supply chain of hacked data, and the tactics used to compromise the websites. I am also building a system for early detection of compromise that can beat blocklisting by Google Safe Browsing by up to ten days.
- **Cloud Watching.** Oct 2022 - Dec 2022
  I studied abuse of rapid IP allocation on Amazon Web Services, Microsoft Azure, and Google Cloud Platform by churning over 60,000 IPs. I identified 650 second-level domains that can be easily taken over by attackers for under $0.01 per domain. I measured the reachability of blocklisted cloud IPs to internet services using Zmap scans. Finally, I proposed an attack to deny service to future tenants by poisoning IP blocklists with IPs.
- **GitHound.** July 2019 - Present
  I built an open-source tool to detect leaked sensitive information across GitHub, earning 950+ stars and over $15,000 in bug bounties (GitHub repository)

LEADERSHIP AND SERVICE

GreyHat Cybersecurity Club at Georgia Tech

- *President* Spring 2021 - Present
- *CTF Captain* Spring 2020 - Spring 2021
- *Team Captain, Collegiate Cyber-Defense Competition* Spring 2019

Palmetto Cyber-Defense Competition

- *Red Team Member* April 2019 - Present (yearly)

TEACHING EXPERIENCE

Georgia Institute of Technology

- **CS 2051 - Honors Discrete Math**, Head TA with Gerandy Brito Spring 2022
- **CS 4540 - Advanced Algorithms**, TA with Gerandy Brito Fall 2021
- **CS 1332 - Intro to Data Structures and Algorithms**, TA with Mary Hudachek Buswell Spring 2020
- **GreyHat Club - Stepping into Security seminar**, Instructor Spring 2020

HONORS AND AWARDS

- **Georgia Institute of Technology** - First Place, Ideas to Serve Spring 2020
- **Georgia Institute of Technology** - 'Thank a Teacher' recognitition (3x) Spring 2020, Fall 2021
- **Clemson University** - First Place Overall, CUHackit 2019 Spring 2020

RELEVANT COURSEWORK

(Graduate) Statistical Machine Learning, Deep Learning, Machine Learning, Graphical Models for Machine Learning, Advanced Network Security and Measurement, Design and Analysis of Algorithms

(Undergraduate) Probability Theory, Statistical Theory, Advanced Algorithms, Combinatorial Analysis

RELEVANT SKILLS

- **Skills:** Apache Spark, Pandas, Docker, Ansible, machine learning, deep learning, web/network security, penetration testing, web scraping, Linux/Windows system administration, Amazon Web Services
- **Languages:** Python (proficient), Java (proficient), Bash (familiar), Node.JS (familiar), Go (familiar)

TALKS AND LECTURES

- **New Frontiers in GitHub Secret Snatching** Aug 2022
  DEFCON 30 Recon Village