Tillson T. Galloway

+1(843) 801-2005 ⋄ Atlanta, GA

tillson@gatech.edu ⋄ linkedin.com/in/tillson ⋄ tillsongalloway.com

RESEARCH INTERESTS

My research focuses on using data mining and machine learning to understand and detect network 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, and then help make them more robust to the attacks. I am also interested in developing *practical* solutions to these problems, bridging academic work with deployable, operational software.

EDUCATION

Doctor of Philosophy in Electrical and Computer Engineering Aug 2022 – Aug 2026 (anticipated)
Georgia Institute of Technology GPA 4.00
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"
  To appear at the 45th IEEE Symposium on Security and Privacy, May 2024

RESEARCH AND WORK EXPERIENCE

Georgia Institute of Technology Aug 2022 – Present
Graduate Research Assistant, advised by Manos Antonakakis *Atlanta, GA*

First author on published work showing how academic and commercial malicious domain classifiers are vulnerable to evasion and data poisoning attacks. These attacks enable an attacker to evade DNS reputation systems with a 100% success rate for under $10. In the process, I built a state-of-the-art DNS-based reputation system using terabyte-scale datasets (passive recursive DNS logs, WHOIS data, BGP announcements, etc.), feature extraction on a 120TB+ RAM and 8000+ CPU Spark cluster, and classification using machine learning techniques.

Corelight, Inc. June 2022 – Aug 2022, June 2023 – Present
Research Intern *Remote*

I created graph-based machine learning models to detect anomalous remote desktop connections, which assist in detecting living-off-the-land techniques and lateral movement 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*

As an undergrad, 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 that runs DNS queries for the ActiveDNS Project.

Facebook, Inc. Aug 2020 - Nov 2020
Software Engineering Intern *Remote*

New Relic, Inc. May 2019 - Aug 2019
Application Security Engineering Intern *Portland, OR*

PROJECTS

- **Abandoned Infrastructure.** June 2023 - Present
  I built a suite of automated scanning tools that scan popularity lists for abandoned infrastructure, then leverages VirusTotal to attribute the infrastructure to popular companies. Since June 2023, I have earned over $40,000 in bug bounties and a million frequent flier points from this system.
- **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.
- **GitHound.** July 2019 - Present
  I built an open-source tool to detect leaked sensitive information across GitHub, earning 1,100+ stars and over $15,000 in bug bounties (GitHub repository)

LEADERSHIP AND SERVICE

Conferences

- *IEEE Symposium on Security and Privacy (external reviewer)* Spring 2024
- *ACM Conference on Computer and Communications Security (artifact committee)* 2023

GreyHat Cybersecurity Club at Georgia Tech

- *President* Spring 2021 - Spring 2023
- *CTF Captain* Spring 2020 - Spring 2021
- *Team Captain, Collegiate Cyber-Defense Competition* Spring 2019

Palmetto Cyber-Defense Competition

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

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

- **CVE-2023-36720** - Microsoft Windows, CVSS Score 7.5 October 2023
- **CVE-2023-36888** - Microsoft Edge for Android, CVSS Score 6.3 July 2023
- **Georgia Institute of Technology** - First Place, Ideas to Serve Spring 2020
- **Georgia Institute of Technology** - 'Thank a Teacher' recognition (3x) Spring 2020, Fall 2021
- **Clemson University** - First Place Overall, CUHackit 2019 Spring 2020

RELEVANT COURSEWORK

(Graduate) Statistical ML, Deep Learning, Mathematical Foundations of ML, Graphical Models for ML, ML on Graphs, 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