Andrew Chang

chang.andrew.23@gmail.com
+1 (919) 780-3457

Website: andrew-chang.me
Chicago, IL, USA

Experienced cybersecurity professional with a strong track record in cloud security architecture, identity and access management (IAM), and penetration testing. Passionate about actively contributing to the cybersecurity community through the development of cutting-edge security tools and methodologies to assess cloud and IAM configurations.

Education

Georgia Institute of Technology

Master of Science in Computer Science 2019 - 2020
Highest Honors, Specialization in Computing Systems

Bachelor of Science in Computer Science 2016 - 2019
Highest Honors, Specialization in Systems and Architecture / Information Internetworks
Certificate in International Affairs

Experience

Lead Cloud Security Engineer Jan. 2023 – Present
Praetorian Security, Inc.

- Leading penetration tests and configuration reviews against cloud environments and applications for external clients; **3,500+ billable hours and >10 critical/high findings**
- Delivering strategic recommendations to key stakeholders regarding the security posture of their digital infrastructure and assets; **>9.5 Net Promoter Score**.
- Developing new methodology and tools to assess cloud and IAM configurations.
- Supporting sales discovery calls as a subject matter expert.
- Providing guidance for junior engineers to solidify their offensive security foundations.

Security Consulting Engineer May 2019 – Dec. 2022
Cisco Systems, Inc.

- Performed offensive security engagements for external clients; **4,500+ billable hours**.
- Developed and maintained Python framework to automate triage of vulnerability scanner alerts in backbone network fabric for Fortune 15 information technology company. **~30k LoC.**

Head Teaching Assistant Jan. 2020 – May 2021
Georgia Institute of Technology

- Developed labs and exams for brand new CS 6264 – System and Network Defenses online graduate course for the top ranked cybersecurity program in the country.
- Labs included: binary exploitation, end-point security with kernel hooks, and Android WebView phishing attacks.

Security Operations Center Analyst May 2018 – May 2019
Georgia Institute of Technology

Analyzed and triaged security alerts raised by campus endpoint monitoring systems by crafting searches in Splunk, FireEye HX, and other in-house solutions.

Select Projects

AzureHound
Extension to existing AzureHound project to enumerate Azure subscription RBAC roles, RBAC role assignments, and service principal assignments. Written in Go, **~4k LoC**.

ScentTrail
Command-line utility to extend an existing Bloodhound Neo4j graph database to identify vertical privilege escalation based on Azure RBAC permissions. Written in Python and Neo4j, **~1k LoC**.

Certifications

Certified AWS Cloud Red Team Specialist	Oct. 2024
AWS Certified Specialty - Security	Jun. 2024
Google Cloud Certified Professional Cloud Security Engineer	Feb. 2024
Certified Kubernetes Administrator (CKA)	Feb. 2023
Offensive Security Wireless Professional (OSWP)	Oct. 2022
Cisco Certified CyberOps Associate	Aug. 2022
Offensive Security Certified Professional (OSCP)	Oct. 2021
Cisco Certified DevNet Associate	Jan. 2021

Publications

Azure RBAC Privilege Escalations: Azure VM — Feb. 2025

Authored article covering covering methods attackers can use to escalate privileges in Azure subscriptions through Azure VM permissions.

Why Azure B2C ROPC Custom Flows Are Inherently Insecure — Nov. 2024

Authored article investigating the default Azure B2C ROPC flow used for token issuance. Specifically, the flow could be abused by creating authorization tokens with arbitrary scopes.

Mnemosyne: An Effective and Efficient Postmortem Watering Hole Attack Investigation System (CCS '20) — Nov. 2020

Developed a browser-based auditing approach for watering hole-based cyber-attacks by overcoming limitations relating to recording necessary semantic information instead of just viewing system calls.

Select Involvements

National Tech Committee Engagements Subcommittee Lead — 2022 – Present
DSA

Crypto Village Volunteer — Fall 2022
Hak4Kidz

Graduate Research Assistant — Fall 2020
Georgia Institute of Technology – Institute of Privacy and Security

Skills

Cybersecurity

- Cloud Penetration Testing
- Secure Cloud Architecture
- Application Penetration Testing
- Network Penetration Testing
- Secure Code Review
- Purple Team Assessment
- Binary Reversing and Exploitation
- Static & Dynamic Malware Analysis
- Security Incident Response
- Wireless Network Exploitation

Cloud

- Microsoft Azure
- Microsoft Entra ID
- Amazon Web Services
- Google Cloud Platform
- Docker
- Kubernetes

Programming Languages

- Bash/CMD
- Powershell
- Python
- C/C++
- Terraform
- HTML/CSS
- JavaScript/TS
- PHP
- Go
- Java
- SQL
- Neo4j
- TeX
- Markdown

Native Languages

- English
- Mandarin Chinese