Nick Gregory

nick@nickgregory.me

INTERESTS

Computer security (especially reverse engineering and binary exploitation), meteorology, photography, bowling.

WORK HISTORY

- Software Engineer, **Google** — Jul 2022 – Present
- Senior Threat Researcher, **Capsule8** (Acquired by **Sophos**) — Jan 2019 – Jul 2022
- Research Intern, **Capsule8** — May 2018 – Aug 2018
  - Researched and implemented strategies to detect zero-day attacks
- MySQL Production Engineering Intern, **Facebook** — May 2017 – Aug 2017
  - Rewrote internal tools used to build out new MySQL clusters
- Research Intern, **M.I.T. Lincoln Lab** — May 2016 – Aug 2016
  - Researched techniques to emulate complete embedded systems in the QEMU hardware emulator

EDUCATION

NYU Tandon School of Engineering, Brooklyn, New York, USA

- B.S. in Computer Science — Sep 2015 – May 2019

OTHER EXPERIENCE

- Vice President & Infrastructure Manager, **NYU OSIRIS Lab** — Sep 2015 – Dec 2018
  - Oversaw most lab research efforts, and managed all lab infrastructure
- Co-Lead, **CSAW CTF** — 2016 – 2018
  - Wrote challenges for, and helped run CSAW CTF
  - During this time, CSAW Finals expanded from 1 site to 5 international locations

TALKS

- Be Kind, Please Rewind: Adventures in creating a macOS record/replay debugger, **REcon** 2023
- Uncommon Sense: Detecting Exploits with Novel Hardware Performance Counters and ML Magic, **Black Hat USA** 2020
- Using Linux Tracing for Security, **CSAW C2** 2019

PUBLICATIONS

- Using Undocumented Hardware Performance Counters to Detect Spectre-Style Attacks, **CAMLIS** 2021
  - Nick Gregory, Harini Kannan
- SoK: Enabling Security Analyses of Embedded Systems via Rehosting, **ACM ASIACCS** 2021
  - Andrew Fasano, Tiemoko Ballo, Marius Muench, Tim Leek, Alexander Oleinik, Brendan Dolan-Gavitt, Manuel Egele, Aurélien Francillon, Long Lu, Nick Gregory, Davide Balzarotti, and William Robertson

PROJECTS

- Introduction to Offensive Security
  - A course I co-created to teach offensive security at NYU
- Dispatch
  - A Python framework for programmatically disassembling and patching binaries
- Weather Explorer
  - A fully open-source website for exploring current weather and forecast data
- Snapshot LKM
  - A kernel module to add a fast snapshot/restore mechanism for fuzzing. Adopted by the AFL++ project.

BUGS

- **CVE-2022-25636** — 2022
  - A kernel heap out of bounds write leading to privilege escalation

ACHIEVEMENTS & AWARDS

- 10th Place, DEFCON CTF Finals (RPISEC) — 2018
- 9th Place, CSAW CTF Finals (NYUSEC) — 2015

SKILLS

C, C++, Go, Python, x86 assembly, ARM assembly, SQL