Rajat Gupta

rgupta415@gatech.edu | Linkedin | Github | rjt-gupta.github.io | (470)883-3124

Education

- **Georgia Institute of Technology** Atlanta, USA
  Doctor of Philosophy in Computer Science; ***Advisor: Dr. Taesoo Kim*** *2022 – Present*
- **Vellore Institute of Technology** Vellore, India
  Bachelor of Technology in Computer Science; ***CGPA: 9.22/10.00*** *2017 – 2021*

Experience

- **Security Research Intern** **Georgia Institute of Technology**
  Advisor: Prof. Taesoo Kim *July'21 – April'22*
  - Collaborated on Systematization of Knowledge (SoK) of Web-Browser Security landscape by performing a 10-year longitudinal study of browser bugs. [Preprint]
  - Gained insights like popular classes of security bugs, exploitation techniques, and the mitigation deployed in four major web-browsers Chrome, Firefox, Safari, and Edge.
  - Analyzed state-of-the-art tools from last 10-years capable of finding critical browser engine bugs using fuzzing and static analysis.
- **Security Research Intern** **University of California, Santa Barbara**
  Advisors: Prof. Giovanni Vigna and Prof. Christopher Kruegel *May'20 – June'21*
  - **Bug Finding -** Found 31 0-days in 212 unique signed kernel drivers while working on automatic detection of Windows Kernel Privilege Escalation bugs using targeted Symbolic Execution.
  - **Framework -** Implemented a 3-stage framework having Scraper Engine, Extraction Engine, and Analysis Engine to detect windows kernel API misusage capable of manipulating privileged memory from Ring-3.
- **Google Summer of Code Student** **The Honeynet Project**
  Mentor: Evgeniia Tokarchuk *May '19 – August '19*
  - Lead the release of an advanced reactive Web Application Honeypot - SNARE/TANNER for the detection and analysis of malicious attacks on web apps.
  - Implemented emulators for vulnerabilities like Template Injection, PHP Object Injection, and XXE Injection etc including building execution environments using custom docker images and php sandbox. [Product Report]

Bug Hunting and CTF

- **Google Chrome:** A mitigation bypass in Turbofan JIT engine (under embargo).
- **Windows Priv Esc:** MSI Dragon Center (CVE-2021-29337) and Intel BIOS update utility (CVE-2021-33104).
- **Defcon CTF Finals 2022:** 5th place with team **perfect r⍟⍟⍟t**
- **Defcon CTF Finals 2021:** 4th place with team **StarBugs**.
- **Defcon CTF Finals 2020:** 7th place as part of **Shellphish**.
- **CyBRICS CTF Finals 2019:** Finished 11th place with team **vitctf**.

Publications

- **POPKORN: Popping Windows kernel drivers at Scale**
  Rajat Gupta, L. Dresel, N. Spahn, G. Vigna, C. Kruegel, and T. Kim. *Proceedings of the Annual Computer Security Applications Conference (**ACSAC**)*, 2022
- **On the Analysis of Web Browser Security Landscape: Vulnerabilities, Trends and Mitigations** (Under Submission)
  Jungwon Lim, Yonghwi Jin, Mansour Alharthi, Xiaokuan Zhang, **Rajat Gupta**, Kuilin Li, Jinho Jung, Daehee Jang, Taesoo Kim

Skills and Interests

- **Languages:** Python, Javascript, C/C++.
- **RE Skills:** Angr, IDA Pro, Ghidra, GDB.
- **Technologies:** CodeQL, Kubernetes, Docker, Git, LaTeX.