Sreehari P J

+91-8590703518 | sreehari.nitt@gmail.com | linkedin.com/in/sreeharipj | github.com/sreeharipj | sreeharipj.github.io

Education

National Institute of Technology Trichy (NITT) — Tiruchirappalli, India
Bachelor of Technology in Instrumentation and Control Engineering — *Aug. 2024 – May 2028*

Technical Skills

Languages: C, Go (Golang), Python, Bash, C++
Systems & Infrastructure: Linux Kernel Internals, eBPF, Docker, AWS (S3, CloudFront)
Security & Tooling: Burp Suite, Wireshark, Ghidra, Nmap

Experience & Security Research

Undergraduate Research Intern – ICS/OT Security — Nov. 2025 – Present
National Institute of Technology (NIT) Tiruchirappalli — *Tiruchirappalli, India*

- Contributing to an IISc-funded project under Dr. Ghanshyam S. Bopche, brainstorming and executing threat models for Indian power grid substations against APT-level ransomware.
- Researched ransomware strains (e.g., DarkSide) targeting ICS environments, utilizing Ghidra and CAPA to analyze execution stages, DLL hijacking vectors, and general encryption behaviors.
- Threat-modeled legacy ICS protocols (IEC 104) to identify trust boundary flaws, currently validating attack trees by executing targeted tests against a lab-provided Software-in-the-Loop (SiL) environment.

Cybersecurity Member — Aug. 2025 – Present
Spider R&D Club, NIT Trichy — *Tiruchirappalli, India*

- Conducting proactive infrastructure audits and red-team engagements across the university's digital and physical network perimeters alongside club peers.
- Identified a Subdomain Takeover on a dangling `nitt.edu` record by correlating DNS anomalies to an external DigitalOcean droplet hosting an Indonesian gambling site.
- Collaborated with the Computer Support Group (CSG) to remediate the hijacked DNS record, which catalyzed a campus-wide policy update prohibiting external IP routing for student bodies.
- Demonstrated a critical physical denial-of-service vector in the central datacenter's CS121 UPS by porting a public authentication bypass exploit (BID-67438) into a custom Bash payload, leading to secured access controls.

Independent Security Researcher — Aug. 2024 – Present
Bug Bounty & Vulnerability Disclosure — *Remote*

- Discovered and responsibly disclosed a critical AWS misconfiguration in a production dating application , securing over 150GB of exposed PII including user media and invoices.
- Conducted manual infrastructure reconnaissance utilizing Burp Suite to identify a misconfigured CloudFront distribution that exposed an unauthenticated S3 bucket directory listing.
- Reported the vulnerability directly to the vendor, leading to the immediate remediation of the exposed bucket, enforcing authentication requirements and preventing automated data scraping.

Projects

REKD: Ransomware Encryption Kernel Detector | *eBPF, C, Go, Python* — Ongoing

- Engineered an eBPF-based ransomware detector utilizing `fentry` hooks on `vfs_write`. Implemented a verifier-safe "scattered read" heuristic in C to sample the head, middle, and tail of file buffers, detecting partial encryption while strictly bounding kernel memory copies.
- Architected a high-throughput Go userspace agent (`cilium/ebpf`) with a decoupled concurrency model; utilized a dedicated goroutine to drain the BPF ring buffer into channels, preventing event drops during I/O bursts while a worker pool handled CPU-bound Shannon entropy calculations.
- Developed a secondary Python/BCC implementation for rapid prototyping and built real-time terminal user interfaces (TUIs) using Bubble Tea (Go) and Rich (Python) for live threat observability.