Nevin Shine

Systems Security Researcher (CS Undergraduate)
Citizenship: German | **Phone:** +49 157 54256832
Nürnberg, Germany | Currently in India (Semester 4)
Email: nevinshine05@outlook.com | GitHub: github.com/nevinshine

RESEARCH INTERESTS

Primary Focus: Kernel-native runtime enforcement, split-plane defense strategies, and targeted intrusion mitigation.
Research Goal: Replacing probabilistic detection with deterministic **eBPF-LSM** state machines to secure Linux runtimes against living-off-the-land attacks, fileless malware, and advanced persistence threats.

RESEARCH EXPERIENCE

Independent Systems Security Research Projects Aug 2025 – Present
Independent Researcher *Remote / Nürnberg*

1. Sentinel Runtime (Kernel Defense) – ***Phase M8 (Active Research)***

- **Architecture:** Designed a custom **eBPF-LSM (Linux Security Module)** enforcement engine to mitigate targeted intrusion and evasion tactics.
- **Innovation ("The Bloodline"):** Implemented kernel-space process-inheritance tracking to neutralize fork-evasion malware and container breakout paths, enforcing strict policy propagation across the process tree.
- **Performance:** Measured **<5 μs overhead** per syscall under stress tests exceeding 10,000 concurrent processes, verifying viability for high-performance environments.
- **Mechanism:** Replaced legacy `ptrace` supervision with ring-0 eBPF hooks (`bprm_check_security`, `task_alloc`) to block unauthorized execution and fileless malware vectors (`memfd_create`) without context switches.
- *Tech Stack:* C (Kernel), eBPF, Clang/LLVM, Linux Kernel 6.8.
- *Artifact:* github.com/nevinshine/sentinel-runtime

2. Hyperion (Wire-Speed Network Containment)

- **Objective:** Designed an **XDP (eXpress Data Path)** firewall to disrupt command-and-control channels at the NIC level.
- **Mechanism:** Performs **O(1)** packet rejection in the network driver, bypassing the OS stack to contain compromised hosts even if user space is degraded.
- **Integration:** Correlates with Sentinel to form a split-plane defense model in which host-level detections trigger immediate network isolation.
- *Tech Stack:* eBPF, XDP, C, Scapy.
- *Artifact:* github.com/nevinshine/hyperion-xdp

3. Project Telos (Agentic Security Architecture)

- **Vision:** A closed-loop enforcement runtime for autonomous AI agents that correlates high-level intent with kernel-level execution graphs to mitigate indirect prompt-injection attacks.
- *Status:* Designing an architectural blueprint for an eBPF-native control plane to study data-exfiltration prevention in autonomous systems.
- *Artifact:* github.com/nevinshine/telos-runtime

PUBLICATIONS & ARTIFACTS

Sentinel M4: Kernel Supervision via Seccomp User Notification Feb 2026
Preprint Technical Report (Legacy Architecture)

- Authored a technical report analyzing the performance trade-offs between the M4 (seccomp user-notification) architecture and the M8 (eBPF) engine, including threat modeling for `io_uring`-based evasion.

TECHNICAL SKILLS

- **Kernel & Security:** Linux Kernel Internals, eBPF (LSM/XDP), Runtime Enforcement (Intrusion Prevention), Kernel Data-Structure Analysis, Malware Kill Chains.
- **Languages:** C (System/Kernel), Python (Automation/TUI), Assembly (Reading), SQL.
- **Tools:** Clang/LLVM, bpftool, GDB, Git, Ghidra (Learning).

EDUCATION

Bachelor of Technology in Computer Science & Engineering Expected 2028
Amal Jyothi College of Engineering, Kanjirappally, India *Current: Semester 4*

- **Focus:** Applied Systems Security, Operating Systems, and Kernel Development.

HONORS & ENGAGEMENT

- **Best Concept Award:** Mar Mathew Vattakkuzhy Award (Mastermind 2025) – *Proposed architecture for Mindscape BCI.*
- **Challenge:** 100 Days of Systems Security (Daily kernel research documentation).
- **Languages:** German (Native), English (Professional/Bilingual).