Nevin Shine

Systems Security Researcher

German Citizen | Nürnberg, Germany (May–Aug 2026)
Currently in India (B.Tech Semester 4)
+49 157 54256832 | nevinshine05@outlook.com | github.com/nevinshine

Research Focus

Area: Semantic-to-Execution gap: enforcing correctness across compiler, kernel, and runtime layers
Thesis: Memory safety and behavioral safety are orthogonal; both must be enforced at different layers
Stack: eBPF/LSM, LLVM/inkwell, AMD-V/KVM, Z3 SMT, Rust, C/C++, XDP, gRPC

Research Projects

Sentinel-CC — Compiler-Kernel Execution Integrity 2026 (Active)

- BFS-based call graph traversal from binary imports reducing syscall attack surface by 81.6%
- Custom LLVM Module Pass extracting syscall provenance and detecting obfuscated patterns
- Cryptographic integrity chain using SHA-256 and Ed25519 verified via Linux kernel keyring
- 25 eBPF hooks enforcing syscall provenance, control-flow integrity, and runtime constraints
- Full red-team validation: 12/12 attack vectors blocked
- Measured overhead: 274ns per syscall (within wire-speed threshold)

Telos — Kernel-Aware Systems Programming Language 2026 (Active)

- Dual-target compilation producing both ELF binaries and eBPF-LSM sandbox enforcement
- LLVM-based pipeline using inkwell for simultaneous BPF and x86 code generation
- Automatic kernel policy synthesis from language-level capability declarations
- Integrated Z3 SMT solver proving memory safety, bounds correctness, and invariants
- Compilation aborts on formal verification failure with counterexample generation

Telos Runtime — AI Kernel Containment 2026 (Active)

- Kernel-level enforcement of AI agent intent against prompt injection and data exfiltration
- Cross-vector taint tracking: sensitive file reads automatically block network access
- Multi-layer domain intelligence pipeline with minimal LLM involvement
- Benchmarked at 100% attack prevention with zero false positives

Sentinel VMI — Hypervisor-Based Introspection 2025–2026

- Hardware-enforced protection using AMD-V Nested Page Tables
- Prevents rootkit modification of `sys_call_table` via #NPF fault trapping
- Reconstructs process state via direct guest memory introspection (BTF-aware)
- Cross-layer integration with runtime and network enforcement systems

Hyperion XDP — Wire-Speed Network Enforcement 2025–2026

- XDP-based firewall performing packet drops before kernel allocation
- Integrated signaling from runtime and hypervisor layers
- Zero-copy telemetry and dynamic reconfiguration without downtime

Sentinel Runtime — Kernel Intrusion Prevention 2025

- Replaced ptrace-based monitoring with seccomp user notifications
- Reduced overhead from 54× to 1.12×
- Defends against io_uring abuse, stealth processes, and TOCTOU attacks

Technical Skills

Languages:	C, C++, Rust, Go, Python, x86 Assembly
Compiler Systems:	LLVM IR, inkwell, custom passes, dual-target compilation
Formal Methods:	Z3 SMT, Hoare logic, symbolic execution, IFC
Kernel Systems:	eBPF (LSM/XDP), KVM, AMD-V, namespaces, seccomp
Security:	Control-flow integrity, taint tracking, policy enforcement, cryptographic validation
Networking:	TCP/IP, XDP, gRPC, Protobuf
Tools:	GDB, strace, bpftool, perf, QEMU, Git, CI/CD

Education

Bachelor of Technology in Computer Science Expected 2028
Amal Jyothi College of Engineering, India

Languages

German (Native) | English (Fluent) | Malayalam (Native)