Uddhav P. Gautam

Ph.D. Candidate in Computer Engineering, Virginia Tech

Raleigh-Durham-Chapel Hill, NC | +1 (919) 729-4141 | upgautam@vt.edu
rgrinnovatellc.github.io | github.com/rgrinnovatellc | linkedin.com/in/uddhavpgautam

Systems researcher specializing in eBPF systems, Linux kernel extensibility, Bluetooth Low Energy security, and secure runtime policy enforcement for resource-constrained embedded devices.

Research Interests

eBPF and Linux kernel systems; embedded and IoT security; Bluetooth Low Energy security; secure over-the-air policy enforcement; runtime monitoring for resource-constrained systems.

Education

Ph.D. Computer Engineering (GPA: 4.0/4.0), Virginia Tech *2024 – Present*
Advisors: Prof. Haining Wang, Prof. Randy Marchany

Ph.D. Computer Science (GPA: 4.0/4.0), UA Little Rock *2018 – 2020*
Transferred to Virginia Tech

M.S. Computer Science (GPA: 3.58/4.0), UA Little Rock *2015 – 2017*

B.S. Computer Science (GPA: 3.91/4.0), Tribhuvan University, Nepal *2009 – 2013*

Publications

Submitted / Under Review

- **Uddhav P. Gautam**. "ZeroDown: A Zero-Downtime IoT Policy Enforcement Framework." Submitted to *ACM WiSec*, 2026.
- **Uddhav P. Gautam**. "BlueSentry: Dynamic Runtime eBPF Policies for Comprehensive BLE Security on Embedded Devices." Under review, 2025.

Peer-Reviewed Publications

- **Uddhav P. Gautam**. "Eliminating eBPF Tracing Over Untraced Processes." *Proc. ACM SIGCOMM Workshop on eBPF & Kernel Ext.*, 2024. DOI: 10.1145/3672197.3673431
- **Uddhav P. Gautam**. "HELOT—Hunting Evil Life in Operational Technology." *IEEE Trans. Smart Grid*, vol. 14, no. 4, pp. 3058–3071, Jul. 2023. DOI: 10.1109/TSG.2022.3222261

Research Experience

Graduate Research Assistant, Virginia Tech *Sep 2023 – Present*

Zero-Downtime IoT Policy Enforcement (ZeroDown Project)

- Designed **ZeroDown**, a zero-downtime post-commissioning policy enforcement framework for MCU-class IoT devices built on a hook-agnostic event-context ABI and an embedded uBPF runtime
- Implemented a secure OTA policy lifecycle with integrity checks, HMAC-based origin authentication, replay protection, crash-consistent A/B slots, and an operator-controlled fail-safe master switch
- Evaluated the framework on Zephyr RTOS and nRF52840, demonstrating a 257KB flash footprint, 128KB RAM usage, 2.25s median BLE GATT update latency (3.1s p99), 0.7ms boot overhead, and 342.3µs per-event runtime overhead
- Demonstrated deterministic runtime policy toggling for BLE pairing enforcement without rebooting or reflashing the device

Bluetooth System/Security Research (BlueSentry Project)

- Designed **BlueSentry**, an application-layer BLE security framework that combines FSM-based enforcement of core invariants with sandboxed eBPF policies for pattern-based D1–D4 threat detection, without kernel or controller changes
- Built a hybrid policy architecture with per-device MAC exceptions, device-class policies, zero-trust defaults, and runtime-tunable timing profiles
- Implemented integrity-verified OTA policy updates carrying runtime flags, thresholds, and eBPF bytecode, enabling security policy evolution without firmware reflashing or service interruption

- Validated host-visible detection of pairing and key-size downgrades, pairing and authentication anomalies, reconnection spoofing, and CTKD weakening on Zephyr RTOS
- Demonstrated deployability on nRF52840 DK with a 291KB flash footprint, 81KB peak RAM usage, and 11,280-byte OTA policy updates completing in 4.4s median

eBPF & Linux Kernel Research

- Published research on reducing eBPF tracing overhead for untraced processes at the ACM SIGCOMM Workshop on eBPF & Kernel Extensions
- Developed kernel-level protobuf parsing by porting the user-space pbtools library into a kernel module and implementing a custom kfunc for in-kernel message processing
- Prototyped a high-performance application-layer firewall using TC clsact qdisc and protobuf payload filtering at kernel speeds
- Built automated KVM-based development infrastructure with Terraform for a multi-researcher systems environment

Critical Infrastructure Security (HELOT Project)

- Published research on operational technology security monitoring in *IEEE Transactions on Smart Grid*
- Designed an end-to-end SCADA monitoring pipeline using GRR, Filebeat, Logstash, and Elasticsearch for continuous event capture and real-time mobile alerting
- Conducted research on runtime security monitoring for DNP3, Modbus, and IEC 61850 environments in power grid infrastructure

Selected Systems Projects

Protobuf-Driven Kernel Firewall

- Ported the user-space protobuf parser *pbtools* into a kernel module with a custom kfunc for BPF integration
- Prototyped a TC clsact-based firewall for application-layer inspection at kernel speeds
- Demonstrated the viability of complex protocol parsing in eBPF programs through kernel-module augmentation

Professional Experience

Android Technical Lead & Architect, Perficient (Client: TD Ameritrade/Charles Schwab) *Jun 2021 – May 2023*

- Architected migration infrastructure supporting the transition of 30M+ TD Ameritrade users across Android, iOS, and web platforms to Charles Schwab systems after acquisition
- Led an 8-engineer Android team, established engineering standards, and maintained architecture and delivery documentation for a large regulated codebase
- Modernized the build and release workflow through Kotlin DSL migration, static analysis integration, and CI/CD improvements for multi-flavor production delivery
- Optimized a shared C++ core and the surrounding mobile performance pipeline, contributing to a measured 40% reduction in crash rate through production telemetry

Sr. Android Developer, Viper Design LLC *Mar 2020 – Feb 2021*

- Built an end-to-end IoT software stack for Shark robot-vacuum products spanning embedded firmware and cross-platform mobile applications
- Applied modular Android architecture, dependency injection, and modern serialization patterns to improve maintainability and testability
- Improved application robustness through performance tuning, code shrinking, crash analytics, and automated testing

U.S. Army *Apr 2019 – Apr 2023*

- Served for four years, developing leadership and operational discipline, and achieved the 96th percentile on the Armed Forces Classification Test

Prior roles: Android Developer, Pontos Solution, Nepal (2012–2015); System Administrator, iDream Pvt. Ltd., Nepal (2008–2012).

Technical Expertise

Systems & Kernel
- eBPF (TC, XDP, tracing)
- Linux kernel development
- C/C++, Rust
- Performance profiling

Embedded & Security
- BLE protocol security
- Zephyr RTOS
- OTA update systems
- SCADA protocols (DNP3, Modbus, IEC 61850)

Software Platforms
- Kotlin, Java, Android AOSP
- Clean Architecture
- Coroutines, CI/CD workflows
- Security tooling (ProGuard, MobSF)

Infrastructure
- Terraform, Docker, Kubernetes
- AWS, GCP, Firebase
- Elasticsearch, Logstash, Filebeat
- Infrastructure as Code

Honors & Awards

- First Place, Complete Societal Award; Societal Impact Award; and Best Graduate Project Award, UA Little Rock
- 2nd Place, TechLaunch Entrepreneurial Competition
- Top-5 Final Year Project, Tribhuvan University