Divye Kalra

dkalra3@jh.edu | +1 4438006625 | Linkedin | Github | Livermore, California | Portfolio

Summary

Cybersecurity graduate student and published researcher specializing in cryptography, vulnerability analysis, and privacy-preserving technologies. Skilled in penetration testing and secure system design. Also experienced in punching a bag of sand.

Experience

Johns Hopkins University & Applied Physics Laboratory (APL) Baltimore, USA
Vehicle Security Researcher (Supervisors: Dr. Anton Dahbura, Dr. Ahmed Abdo, Dr. Ilya Sabnani) *Jan 2025 - Present*

- Integrating C-V2X (Cellular Vehicle-to-Everything) communication into VESNOS, a vehicular security simulation platform, to strengthen Secure Credential Management System (SCMS) and reduce communication latency by 20%.
- Researching cybersecurity and assurance challenges in Connected and Automated Vehicles (CAVs) to strengthen secure vehicular communication.

IITB Trust Lab, Indian Institute of Technology Bombay Mumbai, India
Applied Cryptography Researcher (Supervisor: Dr. Manoj Prabhakaran) *Jan 2024 - June 2024*

- Worked on an Information Security project implementing CASE (Completely Anonymous Signed Encryption) in Rust, reducing encryption overhead by 30% and preparing an open-source release.
- Collaborated with 5+ peers on ECAS (Existentially Consistent Anonymous Signatures), improving signature verification speed by 15%.
- Streamlined onboarding and handover for an ECAS development intern, cutting transition time by 40%.
- Developed 10+ foundational functions to support ECAS, accelerating cryptographic implementation for future developers.

Cyber Security Hub, Macquarie University Sydney, Australia
Confidential Computing Researcher (Supervisor: Dr. Dali Kaafar) *July 2023 - Dec 2023*

- Developed a privacy-preserving fuzzy count querying algorithm using Trusted Execution Environments (TEEs), cryptography, and differential privacy.
- Reduced privacy leakage risk by 30-50% with distributed secure enclaves, replacing centralized data curators.
- Achieved query response times of ∼0.45s (small datasets) and ∼16s (large-scale datasets with 1M records).
- Enhanced query accuracy using Bloom filter encoding, achieving >90% correlation between estimated and true counts.
- Demonstrated security and scalability across real-world datasets (UCI Adult & North Carolina Voter Registration).

Education

Johns Hopkins University Baltimore, USA
Master of Science in Security Informatics *Aug 2024 - Expected Dec 2025*

- Coursework: Software Vulnerability Analysis, Security and Privacy in Computing, Cloud Computing Security, Cybersecurity Risk Management, Network Security, Ethical Hacking, Cryptography

BITS Pilani Hyderabad, India
B.E. Electrical & Electronics and M.Sc. Mathematics *Aug 2019 - Jun 2024*

- Coursework: Data Structures and Algorithms, Operating Systems, Object Oriented Programming, Optimization, Operations Research, Differential Equations (Ordinary and Partial), Graph Theory, Advanced Abstract Algebra, Probability and Statistics, Applied Stochastic Processes, Discrete Mathematics, Functional Analysis, Number Theory, Topology

Projects

- **LLM-Powered Security Code Review Assistant**
  Built AI-powered SAST tool detecting 25+ vulnerability types across 8+ languages with 95% accuracy using hybrid pattern-matching and GPT-4 analysis. Reduced security review time by 60% through automated CVSS scoring and OWASP/CWE/MITRE ATT&CK framework mapping. Engineered RESTful API with 4,799 LOC, supporting multiple LLM providers.
- **AI-Driven Security Operations Center with Intelligent Threat Detection**
  Engineered a real-time SIEM platform for an AI-Driven Security Operations Center using Splunk, Python, and TensorFlow to process over 1000 security events per second, achieving 95% accuracy in anomaly detection and a 70% reduction in false positives. Integrated LLM models for natural language security querying, which decreased the mean time to detect (MTTD) threats by 60%. Further automated threat intelligence enrichment through ML-based alert prioritization.
- **Multi-User Chatroom Application**
  Developed a chatroom using Python's socket and select libraries, supporting 50 users with real-time messaging at ∼150 ms latency. Planned end-to-end encryption to enhance security by 80%.

- **Client-Server Messaging System**
  Built a client-server messaging system for efficient message passing and logging using shared memory. Designed a stateless request-response mechanism for synchronized multi-process communication.
- **Software Security, Reverse Engineering, and Vulnerability Analysis**
  Exploited buffer overflows, format string vulnerabilities, return-to-libc, heap exploits (dlmalloc unlink), ROP, stack pivoting, arbitrary read/write, XSS, Shellshock, SYN flooding, RSA flaws, and Docker escapes. Used Ghidra, GDB remote debugging, SEED Labs, OpenSSL, and Kali Linux for threat modeling, penetration testing, and research.
- **Dirty COW Privilege Escalation (CVE-2016-5195)**
  Exploited Dirty COW to gain root access on Linux via a copy-on-write race condition. Evaluated mitigation strategies like memory write protections and kernel patching.
- **Docker runc Container Escape (CVE-2019-5736)**
  Exploited CVE-2019-5736 in Docker's runc to escape containers and execute code on the host. Assessed seccomp, AppArmor, and runtime hardening for mitigation.
- **Cybersecurity Risk Management and Compliance**
  Conducted risk assessments, threat modeling, and security audits for healthcare and retail, ensuring HIPAA, PCI DSS, and NIST compliance. Identified ePHI and payment security flaws, reducing threats by 70%; recommended RBAC, MFA, IDS, AES-256, and TLS 1.3.
- **Kubernetes Security and Compliance**
  Enhanced Cloud and Kubernetes Security by 60% by designing secure OpenStack architectures and exploiting vulnerabilities such as SSRF, container escapes, Helm v2 tiller exploits, and RBAC privilege escalation. Analyzed runtime threats including Docker-in-Docker (DIND) exploits and crypto-mining containers, developing robust policies with Kyverno and Cilium Tetragon to mitigate multi-tenancy risks, insecure APIs, and runtime misconfigurations while ensuring CIS benchmark compliance.
- **Drone and IoT Security Exploitation**
  Performed comprehensive security assessments on DJI Phantom 3 and Parrot Bebop 2 drones using Wireshark to analyze network traffic, services, and the ARDiscovery protocol. Executed multi-vector attacks, including a Denial-of-Service (DoS) to disrupt communication and terminate video streaming, an Evil Twin attack with Fluxion to capture WPA2 credentials via real-time decryption, and exploited a connection weakness to pull the shadow file to retrieve stored credentials.

Publications and Patents

First Inventor | A Device and Method for a Lightweight Stream Cipher
Indian Patent Published in the *Official Journal of the Patent Office*, Issue Number 49/2023
Co-author | Efficient and Lightweight Data Encryption Scheme for Embedded Systems
Published in *e-Prime - Advances in Electrical Engineering, Electronics and Energy* | Paper Link
Co-author | Machine Learning-Based Prediction of Vanadium Redox Flow Battery Temperature Rise
Published in *Energy Storage* | Paper Link

Skills

Languages: C, C++, Python, Java, Rust, SQL, MATLAB, HTML/CSS
Frameworks/Libraries: FastAPI, Django, Java SpringBoot, JDBC, p5.js, Matplotlib
Softwares/Tools/Skills: Git, Docker, DigitalOcean, Kubernetes, Google Cloud Platform (GCP), Jekyll, PowerPoint, Excel, LaTeX, MySQL, PostgreSQL, Network Analysis, Interpersonal Skills, Problem-solving, Bash/Shell scripting, Source Code Analysis, Threat Modeling, Reverse Engineering, Version Control, VMWare, Cybersecurity Compliance
Security Skills and Frameworks: NIST, ISO 27001, CIS, HIPAA, OWASP, MITRE ATT&CK, CVSS, DNS, Proxy, Firewall, TCP/IP, OSI, UDP, IDS/IPS, SIEM, Zero Trust Architecture, Web Application Security, Secure Software Development Lifecycle (SSDLC), Threat Intelligence, Digital Forensics, Malware Analysis, Incident Response, Identity and Access Management (IAM), Jira, API endpoint security, Single Sign-On (SSO)
Operating Systems: Windows, macOS, Linux (Ubuntu, Kali Linux, KDE Neon)

Certifications and Achievements

Brigham Young University CTF 2025: Participated in Capture the Flag Event
University of New Haven CTF 2025: Participated in Capture the Flag Event
Hack The Box Certified Penetration Testing Specialist (HTB CPTS)
Morgan State - Johns Hopkins Workshop: Presented at a student workshop on CAVs (Connected Autonomous Vehicles)
HopHacks 2025: Participated in hackathon hosted by JHU