HRISHEEKESH DANDEKAR

(267) 881-3189 | hdandeka@andrew.cmu.edu | hrisheekesh-dandekar

EDUCATION

Carnegie Mellon University **Aug 2024 - May 2026**
Master of Science, Information Technology – Information Security Advanced Studies
- **GPA:** 3.76/4.00

Vishwakarma Institute of Information Technology **Aug 2020 - May 2024**
Bachelor of Technology, Computer Engineering with Honors in Cyber Security
- **GPA:** 9.39/10

WORK EXPERIENCE

American Express - Synechron **May 2025 - Aug 2025**
Java Consultant *Weston, Florida*
- Architected a distributed journey-stitching system to correlate heterogeneous event streams from multiple autonomous departments into consistent end-to-end workflows.
- Scaled stitching throughput horizontally by sharding compute across cluster nodes, removing centralized processing and single-thread execution paths.
- Solved distributed locking challenges by leveraging ElasticDB's optimistic concurrency control to implement pessimistic locks.
- Guaranteed correct event attribution despite out-of-order and late-arriving logs, while maintaining high availability during continuous ingestion.
- Delivered the solution in Java, focusing on concurrency control, fault isolation, and correctness under concurrent writes. [Java, ElasticDB]

CrowdStrike **Aug 2023 - Feb 2024**
Security Engineering Intern *Pune, India*
- Engineered kernel-mode C++ probes to inspect and validate Windows IIS security configurations, supporting automated hardening, compliance enforcement, and incident response methodologies.
- Implemented OVAL probes for Windows and macOS, aligning with cybersecurity principles for consistent cross-platform configuration assessments.
- Ensured probe correctness and safety within kernel space, balancing security visibility with system stability and performance constraints.
- Translated industry and internal security hardening standards into executable checks for large-scale enterprise endpoints. [C/C++, Objective-C++]

Post Road Foundation MTEP **Aug 2025 - Dec 2025**
Red Team *Mountain View, California*
- Conducted an authorized red-team assessment of an IoT gateway integrated with inverter, power meter, and thermostat to evaluate real-world attack surfaces and applying network security methodologies.
- Analyzed Modbus-based power meter communications, identifying weaknesses in protocol handling and device trust boundaries to enhance confidentiality, integrity, and availability.
- Achieved privileged access by exploiting bootloader (GRUB) misconfigurations, enabling system inspection and firmware/source analysis, demonstrating information security experience.
- Bypassed LUKS full-disk encryption via a cold boot attack, extracting AES keys from memory under controlled conditions.
- Built and configured a PXE boot environment to reliably capture RAM dumps for forensic key extraction and analysis.

Hacktify Cyber Security **Jul 2023 - Aug 2023**
Red Team *Pune, India*
- Developed CTF challenges, website development, and Udemy course content on security topics, applying ITIL foundation principles to ensure structured content delivery.

Technova Design & Manufacturing **Nov 2020 - Mar 2021**
Project Intern *Pune, India*
- Automated process scheduling for plastic injection molding jobs, optimizing throughput with runtime planning intelligence. [C#, .NET]
- Scavenged and assembled customized PCs at a quarter of market cost.

PROJECTS

Attacking Protocol Intercommunication Gaps **2025**
CMU
- Demonstrated attacks on NFC tap-to-pair by exploiting unauthenticated OOB pairing and Bluetooth multi-connect to impersonate trusted HID devices across iOS, Android, Windows, and macOS.

• Proposed hardware-backed mutual authentication defense.

VishwaCTF Official Website **2024**
• Designed and implemented official website for CMU security CTF.

Image Renderer and BMP Filters in C **2024**
• Developed image rendering algorithms and BMP filter operations using C.

Capstone (Forensics Case) **2024**
CMU
• Analyzed multiple machine images across timezones using digital forensics and recovery tools.
• Defended irrefutability of evidence against other teams in a mock court scenario.

Cyber Heist Security Lab **2024**
• Led a team of 5 in recreating CVE exploits (CVE-2024-47176, CVE-2024-29510) covering buffer overflows, command injections, and Unix printing system vulnerabilities.

AramcoPitt Critical Infrastructure Security Framework Evaluation **2024**
• Applied NIST CSF, STRIDE, FAIR, and OCTAVE (FORTE) to analyze feasibility and implementation for industrial systems.

Network Tunneling Encryption Botnet **2024**
• Created a botnet simulation where compromised machines remain dormant until commanded to launch DoS attacks, communicating via encrypted channels.

SKILLS

- **Programming & Scripting**: Python, C, C++, Go, x86-64 Assembly, ARMv7 Assembly, Objective-C++
- **Binary Exploitation & Reverse Engineering**: GDB, WinDbg, pwntools, Ghidra
- **Cloud & Container Security**: Docker, Kubernetes, Azure Managed Identity, Azure Active Directory
- **Security Frameworks & Standards**: OWASP Top10, NIST CSF, CVSS, MITRE ATT&CK, STRIDE, SOC2, ISO 27001, Cybersecurity Principles, Network Security Methodologies, Incident Response Methodologies, ITIL Foundation
- **Professional Experience**: Information Security Experience, IT Related Experience