Navid Fazle Rabbi

Chapel Hill, NC, USA | navid@unc.edu | 984-369-4148 | navidnaf.com | navid-f-rabbi | NavidNaf
Navid Fazle Rabbi

Objective

With over five years of industry experience in Offensive and Product Security Engineering, I specialize in designing defenses, uncovering vulnerabilities, and developing exploits. My current research centers on hardware security, side-channel analysis, and the intersection of hardware and application security, with an emphasis on delivering real-world impact. Looking ahead, I aspire to drive innovations that strengthen the security of emerging technologies and the systems people depend on every day.

Research Interest

My research interests lie primarily in *Side-Channel Analysis, Reverse Engineering, and Real-world Cryptography*, with a particular focus on bridging the gap between hardware and application security. I further explore challenges in *Offensive Security, including Web and Mobile Application Security, Browser Security, and Source Code Analysis*, as well as emerging directions in *AI Attacks and AI Security*.

Experience

Graduate Research Assistant, Computer Science — *Chapel Hill, NC, US*
University of North Carolina at Chapel Hill — *August 2025 – Present*

- Conducting research on Side-Channel Attacks and Hardware Security by analyzing cryptographic leakage vulnerabilities, contributing to more robust security evaluations across multiple implementations.
- Evaluating Homomorphic Encryption by analyzing side-channel weaknesses in modern applications.
- Researching Keystroke Timing Attacks by evaluating timing patterns in user input to uncover vulnerabilities in secure communication protocols.

Focus: *Side-Channel Attacks, Hardware Security, Homomorphic Encryption, Real-World Applications, Keystroke Timing Attacks, User Input Analysis*

Security Engineer II — *US, UK, BD - Hybrid*
Optimizely Ltd. — *May 2024 – July 2025*

- Improved internal and external security posture by conducting advanced penetration testing and validating findings, which increased remediation of major issues from 10% yearly to 70% yearly.
- Introduced threat modeling to 2 out of 7 products as part of the secure software development lifecycle (SSDLC), which mitigated design-level risks early and reduced the likelihood of high-severity flaws reaching production.
- Advanced DevSecOps maturity by adopting OWASP DSOMM, conducting maturity testing on 30% of products, and integrating SAST/SCA tools from scratch into local and PR-level workflows for 45% of products, enabling early vulnerability detection.
- Built a custom vulnerability management dashboard and developed test code to validate tool (SAST, SCA, ASPM, DLP, SBOM, DAST) performance, which streamlined issue triage time by 40% and enhanced tool effectiveness across security tools.

Senior Researcher, Offensive Security Research — *Dhaka, BD*
bKash Ltd. Portfolio — *April 2021 – April 2024*

- Pioneered a security testing lifecycle for 300+ web applications and 7 mobile applications by focusing on critical, high, and medium vulnerabilities, which ensured timely corrective measures and bolstered overall application security.
- Led red-team operations by simulating APT scenarios and exploiting real-world attack vectors with advanced offensive security tactics, which strengthened organizational cyber resilience and heightened readiness against targeted attacks.
- Discovered and exploited system vulnerabilities by developing custom exploits, performing reverse engineering, malware analysis, and cloud penetration testing across mobile, web, and scalable infrastructures, which uncovered critical weaknesses and advanced defensive strategies.
- Enhanced security posture by implementing compliance frameworks, code sanitization, fraud detection, and cloud security

management, reducing compliance gaps and reinforcing protection against threats.

Education

University of North Carolina at Chapel Hill *Aug 2025 – (ongoing)*
Ph.D. in Computer Science

- **Advisor:** Dr. Andrew Kwong
- **Research Areas:** Side-Channel Attacks, Hardware Security, Web and Browser Security, Hardware–Software (Application) Security Intersection

Islamic University of Technology (IUT) *Jan 2016 – Dec 2019*
B.Sc. in Electrical and Electronic Engineering

- **Advisor:** Dr. Golam Sarowar
- **Research Areas:** Industrial Control Systems (ICS) Security, IoT Security, Secure Communication Protocols, Microprocessor Security, Embedded Systems Security
- **Awards:** OIC Scholarship

Research Highlights

Research Webpage

A Side Channel Analysis of Microsoft Edge Password Monitor Ongoing

Investigating side-channel vulnerabilities in homomorphic encryption schemes and analyzing memory leakage in Microsoft Edge's password monitor to assess practical security risks across modern systems.

Side-Channel Threats to Virtual Keyboard Inputs Ongoing

Exploring side-channel attacks on VR Keyboards by leveraging keystroke timing, cache events, and camera surveillance to infer virtual keyboard inputs and evaluate the security risks of gesture-based interaction.

Design & Analysis of Analog Butterworth and Chebyshev-I Low Pass Filters Preprint

Designed and analyzed Butterworth and Chebyshev-I low-pass filters using approximation methods, Python, and Proteus simulations. Conducted comparative performance evaluation to assess filter efficiency and accuracy in practical applications.
arXiv Link

Design & Implementation of Server Based Position and Angle Measurement and Control of DC Motor UnderGrad Thesis

Developed a Python (Flask) server-based system for real-time measurement and control of DC motor position and angle, integrating hardware design, user interface, and JSON data parsing. Enabled precise dynamic adjustments and reliable server–motor communication, improving control accuracy and experimental efficiency.
Full Thesis

A Security Analysis of Model Poisoning Attacks in Federated Learning Ongoing

Investigating model poisoning attacks in federated learning, analyzing how malicious clients can corrupt global models and exploring effective detection and defense mechanisms to enhance system robustness.

Machine Learning-Powered Threat Detection Framework for attacks in IoT Devices Ongoing

Developing a machine learning-powered framework for effective threat detection in IoT networks. Enhancing security by addressing growing vulnerabilities and improving identification of malicious activity.

Project Highlights

JWT Hawk (JSON Web Token Decoder) Repository

Language: Python
Focus: Built a tool that brute-forces JWT secrets from a wordlist and, on success, decodes and displays the token's header and payload.

The Damn Vulnerable Codebase Repository

Language: C, C++, JavaScript, Python, PHP, Go; Vibe Coded w/ ChatGPT: Ruby, C#, Java, Perl, CoffeeScript, Dart, Scala, Groovy
Focus: Developed a repository of intentionally vulnerable applications across multiple languages for testing SAST and SCA tools, highlighting common security flaws.

C/Cpp Analyzer Repository

Language: Python, C, C++
Focus: Built a Clang-driven analyzer that extracts function metadata (signatures, line ranges), generates call graphs, and performs cross-file function comparisons.

Custom Header (BurpSuite Extension) Repository

Language: Python (Burp Extender API)
Focus: Implemented a Burp Suite extension that adds and modifies custom HTTP headers in both requests and responses using configurable rules and values.

Cookie Monster (Automated Cookie/Session Modifier) Repository

Language: Python, Selenium
Focus: Automated the detection of cookie manipulation vulnerabilities in web applications by simulating user interactions and testing insecure cookie handling.

IceWatch (WebRTC Connection Checker) Repository

Language: JavaScript
Focus: Developed a tool leveraging the RTCPeerConnection API to monitor WebRTC connections, log performance statistics, and track active peer sessions.

Books

সাইবার সিকিউরিটির প্রথম পাঠ **(The First Lessons of Cybersecurity)**
ISBN: 9789843947222
Authored a beginner-friendly book introducing readers to the field of cybersecurity, combining storytelling with practical guidance on security concepts and career opportunities. Designed to be accessible to both technical and non-technical audiences.

Technologies

Languages: Python, C++, C, JavaScript, Bash, SQL, Assembly, PHP

Technologies: IDA, Ghidra, Binary Ninja, R2, objdump, BurpSuite, Git, Browser Consoles and other different penetration testing tools and software.

Notable Certifications

- **Certified Ethical Hacker(CEH)** - EC Council
- **Certified in Cybersecurity (CC)** - ISC2
- **Certified Payment Industry Security Implementer (CPISI) - PCI DSS** - SISA
- **INE Certified Cloud Associate (ICCA)** - INE
- **eLearnSecurity Junior Pentester (eJPT)** - INE

Volunteering

- Serving as a Mentor at the **IUT CTF Club** since June 2023. My primary responsibility is to guide IUT students in Capture The Flag (CTF) competitions. I focus especially on educating them on web application security.
- Serving as a CSSA Officer in the UNC-Chapel Hill Computer Science Department, I act as a bridge between students and faculty by organizing social events, hosting informational workshops, and representing student interests to foster a stronger, more inclusive community.
- Serving as a Security Researcher at the **OWASP® Foundation** since January 2024. I contribute to research initiatives with a focus on Web Testing and the Mobile Application Security Testing Guide (MASTG).
- I am one of the organizers of **BSides Cox's Bazar** and **BSides Dhaka**, and a member of **BSides RDU**.
- Served as Chair of the **IEEE IUT Student Branch** in 2019, Lead Technical Officer in 2018, and Webmaster in 2017.
- Held the position of President of the **IUT Career & Business Society** in 2019, General Secretary in 2018, and Creative Director in 2017.
- Led **Esonance**, the annual departmental electrical fest, as President in 2019 and contributed as Web Developer from 2017 to 2018.