GW | Engineering

# *Revolutionizing the Way We Live, Work, and Learn*

Department of Computer Science

# Letter from the Department Chair

## Revolutionizing the Way We Live, Work, and Learn through *"Engineering AND ..."*

Technology is a catalyst for our rapidly evolving world. At GW's School of Engineering and Applied Science, we make it our mission to positively impact society through the philosophy of *"Engineering and …,"* which puts interdisciplinary collaborations at the forefront of our research and educational activities within the Department of Computer Science. In this brochure, we share some of our proudest moments in the past year when our faculty and students' work integrated technology, healthcare, security, and more.

A cross-cutting theme of our faculty and students' work is improving equity in technological access. This can be seen in both the AI-oriented research of Prof. Robert Pless's group, which aims to ameliorate the shortage of medical professionals in Nigeria by integrating large language models into clinical workflows, and the security-oriented project of graduate student Collins Munyendo, whose work focuses on the unique cybersecurity needs of cybercafe users in Kenya. These collaborations across disciplines and communities worldwide demonstrate the positive, transformational power of computer science.

At the undergraduate level, our students also embody this interdisciplinary spirit, as seen in their participation in the Autonomous Vehicle Competition. By collaborating with peers from other engineering disciplines, they develop practical solutions that fuse technical expertise with creativity and problem-solving.

Another key focus for the department is cybersecurity, with Prof. Sibin Mohan's research on autonomous systems and Prof. Arkady Yerukhimovich's leadership in cryptography and the GW CyberCorps Program playing key roles. These efforts in both research and education prepare the next generation of cybersecurity experts, including students benefiting from NSF and DoD-funded scholarships. Complementing this focus, new faculty members Profs. Shi Feng and Jie Zhou bring cutting-edge expertise in developing safe and secure computer and AI systems.

We invite you to explore how *"Engineering and …"* is shaping the future, blending computer science with diverse fields to create meaningful, real-world impact.

**Rebecca Hwa, Ph.D.**
Professor and Chair
Department of Computer Science
School of Engineering and Applied Science
The George Washington University

## TAILORING COMPUTER SECURITY AND PRIVACY SOLUTIONS FOR UNDERSERVED USERS

Collins Munyendo

In today's digital world, security and privacy threats are worldwide, yet much research tackling them reflects a Western perspective. Recognizing the inequalities this focus perpetuates, the CS Department is expanding traditional research paradigms to better serve and protect all online, exemplified by doctoral student Collins Munyendo's award-winning work on the unique challenges faced by Kenyan cybercafe users.

As Kenya digitizes essential services, cybercafes have become popular internet access points. Munyendo notes that his firsthand experience living in Kenya and visiting cybercafes played a vital role in designing the study and recruiting suitable participants. Through semi-structured interviews with users and managers, he uncovered shared challenges among users, including general computer use and password selection.

Munyendo found that users often seek advice from cybercafe employees, who suggest memorable passwords like national ID numbers, which are easy to guess if bad actors can access their personal information. He recommends alternative methods of authentication better suited to these users' needs, such as password-less options, along with government-provided computer training and security awareness.

By focusing on Kenyan cybercafe users, Munyendo showcases the department's commitment to ensuring technological advancements benefit all communities. His recommendations not only enhance internet safety in Kenya but also emphasize the need to broaden computer security and privacy research beyond Western contexts for a more equitable digital future.

## FRESH FACES, GROUNDBREAKING RESEARCH

Faculty in the CS Department embrace the transformative role of computer science in society, conducting high-impact research that addresses technical and societal complexities while challenging students to do the same. Meet GW Engineering's new minds shaping the future of technology and security, Assistant Profs. Shi Feng and Jie Zhou.

### Prof. Shi Feng »

Dedicated to leveraging artificial intelligence (AI) for the greater good, Feng is at the forefront of AI safety research. His work aims to empower human oversight and inform policy decisions, focusing on the safe deployment of AI systems that could surpass human capabilities. He designs innovative theories, algorithms, and user interfaces to augment human decision-making with and around AI technologies, with recent work investigating the safety risks of using LLMs to support human evaluation and supervision of LLM systems.

### Prof. Jie Zhou »

To transform the design and development of computer systems, Zhou's research focuses on building secure computing systems through principled and rigorous methodologies. He leverages compiler-aided, language-based, and program analysis technologies to enhance the security of systems programming languages and their supporting ecosystems. By championing the philosophy of "building security in," he advocates for integrating security measures directly into software systems during development rather than retrofitting them after production.

# Turning Classroom Learning into Interdisciplinary Triumph

GW's CS-MAE team collaborates to unite algorithm design and deployment mechanisms, highlighting effective teamwork in controlling their aerial vehicle.

Hands-on learning, interdisciplinary collaboration, and a supportive community define the CS Department's approach to preparing students for the working world. Senior design projects are central to this, providing valuable technical, project management, and problem-solving skills. Last academic year, Prof. Timothy Wood enhanced this experience by coordinating participation in the Autonomous Vehicle Competition (AVC) University Innovation Showcase, forming a team of computer science and mechanical and aerospace engineering (MAE) students to enrich their learning further.

Hosted by RTX, AVC challenges students to design and test unmanned vehicles, with teams developing both aerial and ground vehicles. For the first challenge, the CS-MAE team's interdisciplinary skills proved beneficial as it required the aerial vehicle to locate and navigate toward opposing schools' ground vehicles before delivering a water blast to activate a moisture sensor. MAE students designed the deployment mechanism, while CS students developed the target-seeking algorithms. This collaborative development process honed essential project management skills for the students, including budget allocation, material orders, time management, and organization.

Airspace restrictions in Washington, D.C., complicated testing the UAV, leading the team to travel on the weekends to Northern Virginia and Maryland. The CS-MAE Team also faced last-minute challenges at AVC, working overnight to alter the code and adopt a new design that reduces the overall weight and increases the ground clearance to overcome tall grass. Wood notes that having a mix of CS and MAE representation was beneficial for showing these students how both disciplines view and solve problems in different ways.

The GW Engineering team's ability to overcome challenges in preparation for and during the competition earned them AVC's Innovation and Engineering on the Fly Award, highlighting the department's effectiveness in preparing students for real-world engineering challenges. Recognizing the value of diverse skill sets, Wood plans to incorporate electrical and computer engineering students next year to address gaps in soldering and low-level electronics.

Teamwork and innovation shine through as students work late into the night, refining code and designs to tackle last-minute challenges before competition day.

# Integrating Cybersecurity Research, Education, and Workforce Development

The CS Department fosters a robust ecosystem of research and education to tackle today's cybersecurity and privacy challenges. Among the standout faculty is Prof. Arkady Yerukhimovich, whose research and leadership in the GW CyberCorps Program cultivate the next generation of cybersecurity leaders, preparing students for federal service safeguarding national security.

Amid rising threats like ransomware and supply chain exploitation, the department drives research across cybersecurity topics such as cryptography, usable security, and secure system development. Yerukhimovich's cryptography research, in particular, bridges theory with practice, with work in multi-party computation, fake news detection in encrypted messaging, and security analysis of post-quantum cryptography. Supported by the GW Engineering-chartered Cyber Security and Privacy Research Institute, the department is able to extend its impact across GW and beyond.

Through the CyberCorps program, a cornerstone of the federal government's strategy to recruit cybersecurity talent, CS and other disciplinary cybersecurity students benefit from NSF and DoD-funded scholarships to support their education and job placement. Since 2003, the program has graduated over 140 students, boasting a more than 98% placement rate across organizations such as:

The department's location in D.C. further enriches the student experience with unparalleled networking opportunities. Multiple times each semester, students engage with a government official or industry expert to exchange knowledge. Additionally, partnerships with DC-area agencies like NIST enable students, including one of Yerukhimovich's Ph.D. students, to contribute to important national missions during their studies, such as those of NIST surrounding quantum computing advancements.

A core strength of the department and GW CyberCorps program is their recruitment of diverse groups. Over 45% of CyberCorps students are women, and over 15% are from underrepresented minorities. These students are also leaders in student organizations like Women in Cyber Security, which supports women and allies at GW to foster diverse representation within the field.

By integrating research, education, and workforce development, Yerukhimovich addresses today's cybersecurity challenges and ensures CS students are equipped to anticipate and mitigate tomorrow's threats. As threats continue to evolve, the department's commitment to building a strong community of cybersecurity professionals safeguarding vulnerabilities remains vital.

## CyberCorps program by the numbers since 2003

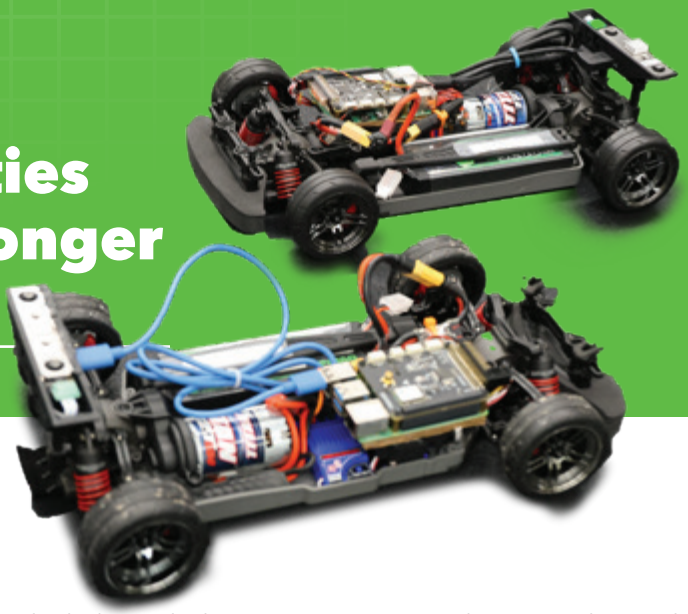
**140+**
students graduated

**98%**
placement rate

**45%+**
students are women

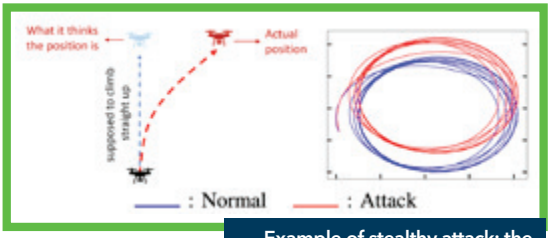
**15%+**
underrepresented minorities

# Exploring Vulnerabilities to Build Stronger Defenses



As autonomous cars, unmanned aerial vehicles, and other autonomous systems become widespread, the escalating reliance on these technologies underscores the importance of ensuring their security, resilience, and efficiency. At GW Engineering, one CS faculty member at the helm of this effort to protect systems in real-time is Prof. Sibin Mohan. Mohan has a diverse research portfolio focusing on various aspects of autonomous system security, with one project exploring the threat landscape to guide their work on advancing system defenses.

While researching threats, Mohan and his student developed the "Requiem" attack, a stealthy attack that exploits the uncertainties in the modeling of autonomous systems–be it from sensor noise, environmental variability, or modeling inaccuracies. By mimicking the system's behavior and weaknesses, these attacks can cause significant mission deviations while remaining undetected. Mohan drew a comparison to scenes in Mission Impossible where Tom Cruise is hacking a system under the nose of the operator, who is unaware since the data determining mission success is still correct.

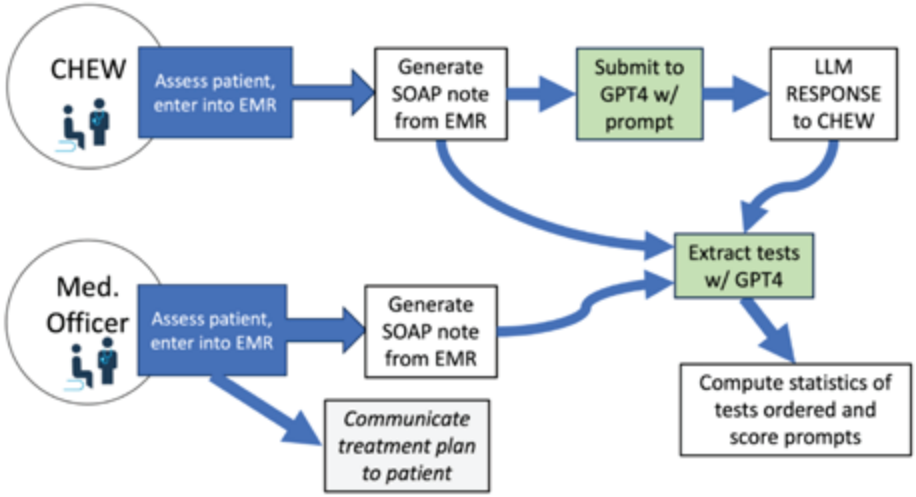



**Example of stealthy attack: the vehicle thinks it is following the mission path** (BLUE) **while in actuality, it is deviating** (RED)**. A realistic example is shown on the right where the attack trajectory is offset to north. Both demonstrate the need to refine its defense.**

Mohan uses machine learning (ML) models, specifically generative adversarial networks (GANs), to develop the Requiem attacks and enhance the system's ability to detect and adapt to threats. This innovative approach allows his team to understand and counter attacks without access to the system's source code, which he has proven effective on a single drone. Taking advantage of GW Engineering's 500,000-square-foot Science & Engineering Hall, Mohan teamed up with an interdisciplinary group of GW Engineering faculty to build the Autonomous Systems Lab, where they will refine their defenses against Requiem attacks and expand to countering attacks on drone swarms.

By understanding attack mechanisms, Mohan's research supports the safe deployment of autonomous systems in critical applications like search and rescue missions. His other ongoing projects around trust-based ML models for autonomous vehicles complement this work, ultimately helping him answer questions about how to detect attacks and protect against harm. As autonomous systems grow in use, Mohan's insights research will undoubtedly play a crucial role in ensuring that these technologies are resilient in even the most demanding situations.

# Leveraging LLMs to Elevate Healthcare in Nigeria




**Schematic of the current study design used to validate their potential scalable solution without exposing patients to risks from the LLM's suggestions.**

Nigeria faces a severe shortage of qualified health personnel, leaving community health workers (CHEWs) with minimal training to assume significant responsibilities, from diagnosing patients to prescribing medicine. To bridge this gap, Prof. Robert Pless and doctoral student Grady McPeak are collaborating with eHealth Africa Clinics to integrate large language models (LLMs) into healthcare workflows and offer "second opinions" for CHEWs.

In dedicated clinics, eHealth Africa offers free consultations where CHEWs treat patients and ask ChatGPT-4 to evaluate the medical record and treatment plan using a prompt designed by Pless and McPeak. Based on the feedback, they may update their plan or suggest further testing. A medical officer (MO) then determines the final treatment plan to ensure patient safety and assess improvements based on AI feedback. Input from CHEW and MO focus groups helped Pless and McPeak design and evaluate 20,000 potential prompts to optimize GPT feedback, highlighting the necessity of computer science skills in handling large datasets.

**Prof. Robert Pless**

Pless and McPeak now prompt GPT to perform a step-by-step assessment of the symptoms, diagnoses, and treatment plans before creating a concise summary. They report that this yields more specific feedback and reduces unnecessary tests, as detailed in 'An LLM's Medical Testing Recommendations in a Nigerian Clinic: Potential and Limits of Prompt Engineering for Clinical Decision Support' (IEEE, 2024). However, bias remains due to the Western-centric nature of LLM training data, with McPeak noting GPT's redundant questions about malaria exposure in Nigeria. Doctors and economists on the project are developing a quality-adjusted life years scale to quantify the improvement in patient lives post-visit, which Pless and McPeak will utilize to compare the effectiveness of LLM feedback in improving treatment plans.

Demonstrating ChatGPT-4's ability to provide feedback mirroring that of a reviewing physician could improve patient outcomes, free high-skill providers for other tasks, and help mitigate the health personnel shortage. Through their involvement, Pless and McPeak are advancing equitable AI use by harnessing the potential of LLMs in low-resource healthcare settings to enhance the lives of vulnerable communities in Nigeria and beyond.

THE GEORGE WASHINGTON UNIVERSITY

WASHINGTON, DC


**School of Engineering and Applied Science**

Department of Computer Science

800 22nd Street, NW
Suite 4000
Washington, DC 20052

**cs.engineering.gwu.edu**

202-994-7181

gwuengineering

gwuengineering

gwuengineering