Facilities, Equipment & Other Resources

NYU Tandon School of Engineering has a distinguished history of research and education in the field of cybersecurity. We have been designated an NSA Center of Excellence in Information Assurance, a Center of Excellence in Research, and a Center of Excellence in Cyber Operations, and are proud to be among very few schools to get all three designations.

1. Facilities

The OSIRIS Lab. With an NSF grant, NYU Tandon School of Engineering launched its cyber security program in 1999, establishing the school's Information Systems and Internet Security Lab and initiating a sequence of undergraduate courses in computer network security. This student-run lab, formerly known as ISIS, has been operating successfully for over 25 years. Today, OSIRIS focuses on four main activities: competing in CTFs under team NYUSEC; running weekly Hack Night workshops that teach cybersecurity topics, tools, and skills; organizing CSAW CTF, a two-round global competition each fall; and industry engagement events with researchers and industry professionals. The collaborative spirit of OSIRIS attracts many students to prefer its dynamic environment over private study areas. Several current SFS scholars are active members of the Lab.

Center for Cybersecurity. Recognizing the importance of interdisciplinary approaches in cybersecurity, NYU Tandon established the Center for Cybersecurity (CCS) in 2009. The center synergizes complementary expertise, faculty innovation, and enthusiasm of students from various NYU schools to advance knowledge and practical applications in security and privacy. CCS encompasses contributions from faculty across multiple disciplines, including Tandon (Engineering), Law, Steinhardt (Ethics, Philosophy, Education), and NYU Abu Dhabi (Engineering). In 2010, CCS won an NSF IGERT grant to fund 24 interdisciplinary PhD students. Today, CCS supports more than 60 PhD students with a team of 25 researchers. With a 10,000 sq. ft. floor designated to CCS, we have a shared space for faculty, post-docs, visiting scientists, PhD students, SFS students, and undergraduates, promoting a dynamic ecosystem that encourages interaction and interdisciplinary collaboration among a diverse academic community.

Collectively, the CCS faculty can boast of 4 NSF CAREER awards, 3 Jacobs Excellence in Education awards (NYU Tandon faculty honor), 2 "Brilliant 10 under 30" awardees from Popular Science magazine, 2 IEEE fellows, and 1 "Outstanding Researcher" award from Intel. In collaboration with a cadre of gifted graduate students, the faculty routinely present at top-level conferences on topics ranging from privacy protection to securing hardware elements and software supply chains.

Since the establishement of CCS, our cybersecurity research activities have seen significant growth, having received over $64 million in research and education funding for security-related research. Research specializations include: AI and Cybersecurity; Cybercrime; Cyber Governance & Strategy; Digital Forensics; Disinformation and Deepfakes; IoT Security and Privacy; Manufacturing Security; Privacy and Data Protection; Securing Cyberphysical/Communications Systems; Software and System Security; and Supply Chain Security.

As the primary hub for cybersecurity research at the university, CCS hosts several faculty-led labs where

SFS students engage in project work. These include:

Secure Systems Laboratory. Under the direction of Justin Cappos (PI), the lab works to find practical and deployable solutions to real-world security threats. Over the past few years, the lab has developed products and improved on existing system designs that detect and isolate security faults, secure private data, provide a secure mechanism for fixing software flaws in different contexts, and even foster a deeper understanding about how to help programmers avoid security flaws in the first place. The overarching theme of the group is to solve research problems in a practical manner and deploy these solutions into production use. SSL's current work focuses on security, virtualization, cloud computing, crypto, and IoT. They have developed several pieces of open source software that have millions of users. The software is used in production by git, Microsoft, IBM, RedHat, Docker, Python, many automakers, and most Linux distributions. Their TUF project, a secure software update framework, is used on millions of devices through integrations in dozens of cloud vendors including Docker, IBM, Microsoft Azure, RedHat, and VMware. The TUF project is now hosted by the Linux Foundation under the Cloud Native Computing Foundation. The followup work on Uptane, which is undergoing IEEE/ISTO standardization, has been adopted by automakers for nearly one-third of the cars on US roads to provide a secure over-the-air solution for updating software in automobiles. The lab's security architecture for git was adopted into git in September 2016.

The Laboratory for Agile and Resilient Complex Systems (LARX). Led by Prof. Quanyan Zhu, the research activities of the LARX lab focus on developing fundamental principles and tools for secure, resilient, and sustainable dynamical systems and networks. These tools have applications to communication networks, cyber-physical systems, and modern critical infrastructures, smart energy systems, and human-in-the-loop systems. Interdisciplinary by design, the LARX team collaborates with faculty members and graduate students in the Power Lab, Wagner Graduate School of Public Service, Laboratory for Entrepreneurship in Data Sciences at NYU, and with other outside research institutes. Its work is currently funded by government agencies such as the National Science Foundation (NSF), and NYU's Center for Advanced Technology in Telecommunications (CATT).

EnSuRe (Energy-aware, Secure and Reliable Computing Research) Lab. Led by Prof. Siddharth Gard, EnSuRe hosts 10 PhD students, and 2 Postdocs. The group describes its research as being "at the intersections of computer hardware design, cyber-security, and machine learning, with a particular focus on computer hardware," including electronic design automation and micro-architectural solutions.

The Machine Learning, Embedded Systems and Software/Systems Security (MESS) Lab is one of the newest research labs affiliated with the Center for Cybersecurity. Under the direction of Prof. Brendan Dolan-Gavitt, the lab hosts 8 PhD students and works on such issues as software security, vulnerability injection, and the security challenges of embedded devices. The lab also collaborates with the Secure Systems Lab on a virtual machine design that limits interactions with an operating system kernel to only commonly-used code, and with the EnSuRe lab to investigate backdoors in deep neural networks.

The mLab, under the direction of Prof. Danny Yuxing Huang, is dedicated to identifying and thwarting real-world security and privacy threats, particularly those related to the use of smart devices on the Internet of Things. The "m" in its title reflects the team's commitment to using empirical measurements

to allow non-technical consumers to assess potential security issues with their smart home IoT devices. The lab also develops new methods to thwart cybercrime, such as tracing millions of dollars worth of cryptocurrency transactions of criminals, such as ransomware. mLab houses 10 students–5 PhDs, 2 Masters, 1 Undergrad, and 2 High Schooler–and is funded by an NSF award on IoT network measurement, an NSF award on IoT usable privacy, Consumer Reports Digital Fellowship, Google CYber NYC Ward, and JP Morgan Faculty Research Award. The lab is contracted by various government agencies from the FBI to the New York State Attorney General to help with the investigations of a number of security and privacy threats related to its research and its work has been covered in multiple media outlets such as the New York Times, NPR, BBC, The Washington Post, and TechCrunch.

2. **Resources**

Cybersecurity for Democracy is a research-based, nonpartisan, and independent effort to expose online threats to our social fabric – and recommend how to counter them. This project is a multi-university research of the Center for Cybersecurity at the NYU Tandon School of Engineering and the Cybersecurity and Privacy Institute at the Northeastern University Khoury College of Computer Sciences. The project uses traditional cybersecurity methods to evaluate vulnerabilities of online platforms that are used to spread misinformation. It focuses on systems, revealing the ways that online sites leave themselves open to misinformation attacks, and develops mitigation strategies to improve online security, working with advocates, policy makers, and platforms.

CSAW Cybersecurity Games & Conference. CSAW is the world's most comprehensive student-run cybersecurity event. It serves as an engaging platform for experiential learning and aims to inspire students to pursue education and careers in the field of cybersecurity. Formed in 2003 as a small local competition by the students of Professor Nasir Memon, co-founder of NYU Tandon's cybersecurity program and former SFS PI, CSAW has expanded to competitions hosted by 5 global academic centers with nine distinct cyber competitions that continuously evolve to meet the changing threat landscape. CSAW plays a crucial role in helping defenders stay updated with these changes, contributing to the development of awareness, proficiency, and innovation in the field of cybersecurity. Celebrating its 21st year in 2023, CSAW has become the largest student-run event of its kind. It attracts the brightest students from around the world, ranging from high school to doctoral candidates. PI Justin Cappos previously served as the faculty lead for the Applied Research competition, which is now led by Co-PI Danny Huang.

Graduate and Undergraduate Cybersecurity Curriculum. Students benefit from a flexible curriculum tailored to their diverse majors and backgrounds. Recognizing the need for individualized approaches, our programs allow for personalized study plans, developed through collaboration between the student, academic advisors, and faculty members.

The graduate cybersecurity curriculum at NYU offers 17 courses, covering fundamental knowledge and practical skills through lab and project work. Popular selections include Penetration Testing and Vulnerability Analysis, Digital Forensics, Offensive Security, Applied Cryptography, and Application Security. Additionally, there are 17 computer science courses available. Most of these courses are also accessible to undergraduates, either as cross-listed options or through enrollment with instructors'

permission. Within the Computer Science Department, the cybersecurity course enrolls nearly 1500 seats, highlighting the program's popularity and relevance.

For undergraduate students, NYU Tandon offers a minor in cybersecurity, requiring a minimum of five courses, including Computer Networking, Computer Security, Network Security, Application Security, and one elective such as Penetration Testing or Applied Cryptography.

Students pursuing a BS or MS in Computer Science, Cybersecurity, or related technical degrees are required to take a minimum of five cybersecurity courses. The majority of students pursuing an MS in Cybersecurity typically take ten courses.

Students pursuing an MS in Global Security, Cybercrime and Conflict complete coursework in Cyber Law, Cyber Power and Global Security, Infrastructure Security and Resilience, Mission Assurance, and Cyber Organizations, plus four technical electives through Tandon's Cybersecurity program.

Non-engineering graduate students from disciplines such as Global Security, Cybercrime and Conflict mentioned above, or Law are required to take at least four cybersecurity courses, supplemented by non-technical security-related courses. Prerequisite courses in programming and algorithmic thinking may be required for non-engineering students and are often completed in the summer before starting their program (see Tandon Bridge Program below).

Online and On-Campus Cyber Security Master's. NYU faculty members have embraced virtual instruction, offering in-person as well as online courses that deliver high-quality education and engaging students everywhere in the world, 24/7. The entire Master's in Cyber Security is available online to both remote and on-campus graduate students. Online cyber security students enjoy a rare level of access to a virtual research laboratory where they can perform hands-on experimentation to reinforce concepts learned in virtual lectures. Students participate in real-time discussions, stimulated by chat, texting, forums and other media. Remote-learning students include personnel from Fortune 500 companies such as Science Applications International Corporation (SAIC), Goldman Sachs, Microsoft, and Google. Additionally, NYU Tandon offers a Cyber Fellows Scholarship, a program that provides scholars with a 75% tuition discount and a flexible schedule. With a fully online, part-time format, students can remain employed as they pursue Master's degrees, directly applying the skills they acquire to their current positions.

The Tandon Bridge Program

The former PI, Nasir Memon, started the Bridge to Tandon Program in 2011 as a means to prepare students from non-STEM backgrounds for graduate level study in a technical program, such as cybersecurity. Bridge is a low-cost, non-credit, fully online program taught by NYU Tandon computer science faculty and covers complex topics such as discrete math and principles of operating systems. Students complete a 28-week asynchronous format, which includes interactive online modules, live webinars, assignments, and exams. Bridge tuition is $1850 total and very affordable compared to similar bootcamps and certificate programs.

Bridge has been an excellent feeder for the SFS program. Two of our recent Bridge to MS students are Reagan Bachman and Dominique Eberhard. Reagan just graduated with her MS Cybersecurity degree (May 2024) and has been hired as a Special Agent by the FBI. Dominique Eberhard, MS Computer

Science (May 2025), is completing an internship with CISA in Summer 2024.

NYU's Wasserman Center for Career Development. SFS students benefit from regular access to career counselors at the Wasserman Center, who assist with application processes and interview preparation. Given the critical timelines of intelligence agency internship applications in September and October, we ensure that students are prepared early in their program. To facilitate this, SFS scholars attend their first session with a career counselor who specializes in federal employment shortly after joining the program.

SFS Study Room

Our SFS scholars have exclusive access to a private study room in a central location at the Center for Cybersecurity, which becomes a central spot for studying and socializing. Anecdotal evidence suggests that students who study together tend to perform better, especially in challenging courses like Cryptography and Application Security. We also organize at least one social activity per semester.