PRESS OFFICE • 1 MetroTech Center, 19th Floor, Brooklyn, NY 11201
CONTACT • Karl Greenberg
646.997.3802 / mobile 646.519.1996
Karl.Greenberg@nyu.edu

Note: Images available at
https://nyutandon.photoshelter.com/galleries/C0000DKT3j1lAvpA/G0000wdarjcpWEXw/CSAW-2019\

Immediate Release

Wednesday, September 25, 2019

At CSAW 2019, virtuous hackers take on

AI, 3D printing, deepfakes, and more

The world's most comprehensive student-led cybersecurity contest, featuring a record nine competitions and six global regions, prepares to tackle new cyber threats

BROOKLYN, New York, September 25, 2019 –The world's most comprehensive student-led cybersecurity contest, the New York University Tandon School of Engineering's annual CSAW games, on **November 6-8, 2019** at NYU Tandon's Brooklyn campus and at academic sites across three continents, is expanding to include new challenges that address vulnerabilities in artificial intelligence (AI) systems, microchip theft, and more.

Since its launch in 2003, CSAW has evolved to address vulnerabilities in new and advancing technologies. In 2018, CSAW introduced Hack3D, which serves to raise awareness in both scientific and manufacturing communities about the need for anti-counterfeiting methods in 3D printing. The high school competition Red Team, which once covered only forensic skills, began offering a taste of how corporations and institutions train defenders for real-world attacks.

Two new CSAW competitions debut this year:

HackML explores vulnerabilities in machine Learning systems, which include such applications as facial recognition, digital assistants, voice recognition, computer vision, behavioral algorithms, and neural networks, and are predicted to generate $190 billion in global business by 2025. Research at NYU Tandon and elsewhere shows that just as with software and integrated circuits, malefactors can install backdoors in machine learning architecture, allowing attackers to trigger malicious behavior. The

HackML competition, **the first of its kind**, will challenge teams of undergraduates and graduate students to design new, powerful backdoor attacks on machine learning systems and to develop novel defenses and detections.

One challenge requires competitors to design a backdoor attack that will allow the attacker to add a visual "trigger" to the image of a human face, causing the back-doored network to incorrectly classify the image as whatever the attacker wishes it to "see" (a hat instead of a face for instance.)

Logic Locking Conquest, funded by the National Science Foundation (NSF), centers on a revolutionary technique for protecting Intellectual Property of integrated circuits from myriad security threats, such as reverse engineering, overbuilding, piracy, and hardware Trojan insertion. Participants will attempt to attack designs locked with state-of-the-art methods.

The scale of CSAW, in this, its 16th year, is evident in its global reach and number of competitive events:

- CSAW US-Canada at NYU Tandon in Downtown Brooklyn, New York will host nine events
- CSAW India at the Indian Institute of Technology, Kanpur (IIT Kanpur) — four events and its annual hands-on "IoT Security Village"
- CSAW Europe in Grenoble-INP Esisar in Valence, France — four events
- CSAW MENA (Middle East and North Africa) returns to NYU Abu Dhabi — four events
- CSAW Israel at Ben-Gurion University and the University of Haifa in Israel (with IBM Research-Haifa and the IBM Cyber Security Center of Excellence) — two events
- CSAW Mexico, in its second year at Universidad Iberoamericana (Ibero) in Mexico City — two events

"For 16 years CSAW has adapted and grown to address changes in the threat landscape for cybersecurity. Fast-evolving technologies like AI and additive manufacturing constitute new battlegrounds where defenders have already faced attacks," said Ramesh Karri, director of CSAW, professor of electrical and computer engineering at NYU Tandon, and co-founder and co-chair of the NYU Center for Cybersecurity. "Events like HackML and the Logic Locking Conquest are not just stimulating competitions; they generate avenues of inquiry, innovative approaches to thinking about devices we use every day, and real-world solutions. Furthermore, competitions like the CSAW Red Team Challenge have encouraged thousands of students to pursue fields with high demand for new talent and fresh ideas. We are especially gratified that CSAW has inspired students who may have never have considered STEM fields otherwise to pursue engineering, math, and science."

Other Events

Hack3D raises awareness and generate discussion in engineering and research communities about security in the additive manufacturing (AM) field. In the qualifying round of this NSF-supported challenge, competitors reconstruct a corrupted G-code file (which tells a machine tool what kind of action to take), employing skills in file forensics and reverse-engineering. During the final round, teams will compete in hacking an anti-counterfeiting system designed to protect CAD models.

Capture the Flag (CTF) lets players of all levels and ages from around the world test their hacking and protection skills. After a grueling 48-hour preliminary competition, finalists compete on-site at one of the six global regions. The 2019 Qualification Round had more than 2000 teams register from 88 countries.

Red Team Competition, NYU Tandon's CSAW high-school competition has introduced thousands of students to cybersecurity. Last year, more than 650 teams competed, with 28 teams winning coveted slots at the CSAW final rounds at NYU Tandon, Ibero, and Grenoble INP-Esisar. The 2019 competition centers on a fictive information security department in a large city.

Embedded Security Challenge, the oldest and largest hardware hacking competition in the world, now in its 12th year, is also the most difficult event at CSAW and contributes to worldwide scholarship. The tournament employs a "red team, blue team" format that mimics real-world attacks. This year's challenge, developed in partnership with the University of Delaware, focuses on the security of radio frequency identification (RFID) readers, which are used in everything from key access control devices in buildings to user authentication in computing systems. This challenge will task contestants with hacking the firmware of a custom RFID card reader using reverse engineering tools developed by the **United States National Security Agency (NSA)**.

The **Policy Competition** at NYU Tandon attracts students who are interested in the nexus of law, policy, and emerging security issues. This year's topics are cyberwarfare, data security, and law enforcement investigations. Finalist teams present their best policy arguments to a panel of judges.

Applied Research accepts only peer-reviewed security papers that have already been published by scholarly journals and conferences. This year, top academics and practitioners will review more than 150 papers to arrive at the list of finalists. Student authors will present their work in poster format to judges. Finals will be held at NYU Tandon, Grenoble-INP Esisar, IIT Kanpur, and Ben-Gurion University.

Security Quiz Bowl lets finalists from other CSAW contests as well as students from the New York City region test their knowledge of security technology, history, and culture in this fun and fast-paced competition, leading up to a final round that will follow on the heels of all final competitions at NYU Tandon. Quiz Bowl is sponsored and hosted by IBM this year.

Industry Fair

CSAW finalists and vetted computer science students from across the region will meet sponsors recruiting for internships and career positions. The worldwide shortage of cybersecurity talent makes the CSAW finalists particularly attractive to elite companies: According to research by industry group (ISC)2, the shortage of cybersecurity professionals is close to 3 million globally. In the United States, there are nearly half a million unfilled positions.

Cybersecurity students wishing to participate in the CSAW Career Fair at NYU Tandon can learn how to submit resumes at https://csaw.engineering.nyu.edu/global/nyu-tandon/agenda/industry-fair

Speakers and Professional Conference

For 15 years, CSAW has brought students in contact with security professionals and their peers so they might build networks of cybersecurity mentors and colleagues for their future careers. This year, the NYU Tandon's student-led Offensive Security, Incident Response and Internet Security (OSIRIS) laboratory will host the C2 Security Workshop, sponsored by BAE Systems. This one-day, 6-session workshop will feature industry speakers addressing a host of hot-button topics in cybersecurity from quantum systems to protocol reversing in RF. For more information and tickets, please see: https://csaw.engineering.nyu.edu/global/nyu-tandon/c2workshop

About CSAW

The CSAW games, founded in 2003 as a small contest by and for NYU Tandon students, have grown to become the most comprehensive set of challenges by and for students around the globe. NYU students continue to design the contests under the mentorship of information security professionals and faculty. The OSIRIS lab, home to weekly student-led Hack Night training and student research, leads the Red Team and CTF challenges.

"Although over 100,000 high school and college students have participated in CSAW over the past 16 years , it is much more than a global competition," said Jelena Kovačević, dean of NYU's Tandon School of Engineering, "CSAW is a cybersecurity bellwether, examining attack-and-parry scenarios being played out across the world today, and exploring new vulnerabilities in areas like machine learning, 3D printing and integrated circuits that may not yet be on defenders' radars. Additionally, CSAW engages students, ignites research and ultimately supports the community, not least because of its role as a creative force in our school-wide commitment to STEM education. Congratulations once again to NYU student team leaders and faculty for ushering in CSAW for its 16th year."

CSAW US-Canada Sponsors are: Gold Level – Army Research Office, Capsule8, and DTCC; Silver Level – BAE Systems, IBM, Red Balloon Security; Bronze Level – Facebook, Flatiron Health, JPMorgan Chase & Co., RiskEcon Lab for Decision Metrics @ Courant Institute of Mathematical Sciences, T. Rowe Price; Supporting Level — Bank of America; Contributing Level – Aflac, Applied Computer Security Associates, CTFd, Datadog, Raytheon, and Uber.

For more information, visit csaw.engineering.nyu.edu, view a video of CSAW highlights, and follow @CSAW_NYUTandon.

About the New York University Tandon School of Engineering

The NYU Tandon School of Engineering dates to 1854, the founding date for both the New York University School of Civil Engineering and Architecture and the Brooklyn Collegiate and Polytechnic Institute (widely known as Brooklyn Poly). A January 2014 merger created a comprehensive school of education and research in engineering and applied sciences, rooted in a tradition of invention and entrepreneurship and dedicated to furthering technology in service to society. In addition to its main location in Brooklyn, NYU Tandon collaborates with other schools within NYU, one of the country's foremost private research universities, and is closely connected to engineering programs at NYU Abu Dhabi and NYU Shanghai. It operates Future Labs focused on start-up businesses in downtown Manhattan and Brooklyn and an award-winning online graduate program. For more information, visit http://engineering.nyu.edu.

###

www.facebook.com/nyutandon @NYUTandon