Editors' notes: Images available at
https://nyutandon.photoshelter.com/galleries/C0000DKT3j1lAvpA/G0000FEgK1ZUjxFI/2019-CSAW-Winners-Release
The full list of Canada-U.S. winners and photos available upon request

Immediate Release

World's most comprehensive student cybersecurity games

announce winners of CSAW 2019

Best young hackers and protectors converged at NYU Tandon School of Engineering and academic hubs in France, India, Mexico, and the Middle East to test their skills in new and dangerous realms of cyberspace

BROOKLYN, New York, Tuesday, November 12, 2019 — CSAW, the world's most comprehensive student-led cybersecurity competition, announced the winners of last week's final rounds, which pressed the globe's most accomplished security students to the max with contests that reflected the real world's rapidly changing threat landscape.

CSAW started as a contest for New York University Tandon School of Engineering students nearly two decades ago and has since grown to include simultaneous final competitions at schools in France, India, Israel, the United Arab Emirates, and Mexico.

And although Capture the Flag (CTF) remains the perennial big draw, CSAW this year continued its tradition of employing contests to advance research in areas of cybersecurity that few have yet explored. The world's first machine learning and logic locking (circuit security) contests debuted, joining others that pushed the boundaries of 3D printing security and embedded systems security (another vital hardware field).

NYU Tandon welcomed 66 finalist teams from the United States and Canada in a record nine competitions, while another 114 teams competed at the other academic hubs.

-more-

As always, this year's CSAW was a contest by students for students: At the Brooklyn hub alone, 34 students from both NYU Tandon's student-led Offensive Security, Incident Response and Internet Security (OSIRIS) Laboratory, the NYU Center for Cybersecurity, and the NYU College of Arts and Sciences worked as competition leads, devising and honing the international games with the help of 100 professionals. Another 64 students volunteered in Brooklyn to run the annual games, now in their 17th year, and events there were supported by 24 industry and government partners.

To earn spots in the coveted final rounds, this year's contestants bested 1,225 teams from 90 countries. At the finals for the United States and Canada, students won cash prizes, and NYU Tandon offered more than $1 million in scholarships to high school competitors. Additional prizes were awarded to contestants at the other academic hubs.

"As a global event attracting the world's best and brightest to test their skills at prestigious schools around the world, CSAW is a global driver of cybersecurity competence, knowledge, and potential for a world grappling with massive technological change," said NYU Tandon Dean Jelena Kovačević. "The expansion of CSAW — from just 50 of our students in 2003 to today's worldwide engagement — illustrates the dedication of NYU Tandon professors, students, and alumni, of whom we are incredibly proud."

Added NYU Tandon Professor Ramesh Karri, the faculty leader for both CSAW 2019 and its sponsoring research center, the NYU Center for Cybersecurity: "The finalists' creativity, dedication, and mettle put them on a trajectory to become leaders in a field whose importance to our institutions and economies cannot be overstated. Our congratulations go out to them and to the faculty and mentors who encouraged and helped educate them."

Capture the Flag

The flagship event of CSAW, CTF, organized by students of the NYU Tandon OSIRIS Lab, gathered finalists who bested 559 teams from around the world to face off at six international CSAW hubs. The notoriously difficult final round demanded a profound understanding of the roles and ramifications of cybersecurity and covered pwning, reverse engineering, web, cryptography, and forensics.

Winners of the US-Canada CTF finals at NYU Tandon were:

- First place: team **perfect blue**, a multi-school team whose members from the University of Waterloo, Purdue University, Drexel University, and the Georgia Institute of Technology met as high school contestants at the CSAW finals two years ago. The team also won the CSAW Security Quiz Bowl and placed second in a side competition called Pwny Racing.
- Second place: team **Sice Squad**, comprising competitors from the University of Pittsburgh, Carnegie Mellon University, the Massachusetts Institute of Technology, and the University of Maryland. It took third place in Pwny Racing.
- Third place: team **PPP**, from Carnegie Mellon University, which also placed second in the CSAW Security Quiz Bowl.

Pwny Racing was designed and hosted by CSAW contributing sponsor Vector35. It was high drama as teams competed in a single-elimination bracket event with each pair of contestants racing to solve a

custom challenge. Students competing as team Kernel Sanders from the University of Florida began as the lowest seeded team, then worked their way from the lowest [bracket](#) to victory. A video of the final round can be viewed at www.youtube.com/watch?v=lYLbwayCzps&t=31574s.

Another side contest came from Red Balloon Security, which filled a real ATM with $2 bills for its **jackpotting challenge**, in which CSAW participants attempted to hack the machine (without damaging it) to make it dispense nearly $2,000. Red Balloon uses just such tests to evaluate job applicants.

Red Team Competition

In keeping with tradition for this high school competition, the challenge imitated real security exercises, this time requiring teams to conduct penetration testing of a fictional city and all its services to discover criminal activities.

- First place: team **b1c**, Montgomery Blair High School, Silver Spring, Maryland
- Second place: team **let down**, West Windsor-Plainsboro High School, North Plainsboro, New Jersey
- Third place: team **bluepwn**, Bellevue, Washington

Embedded Security Challenge

This year's version of the oldest and largest hardware hacking competition in the world, now in its 12th year, centered on the ubiquitous radio frequency identification (RFID) readers. Designed by students and their mentors at the University of Delaware, it employed reverse engineering tools developed by the U.S. [National Security Agency](#) (NSA).

- First place: team **Shellphish**, the University of California Santa Barbara
- Second place: team **pwndevils**, Arizona State University
- Third place: team **Kernel Sanders**, the University of Florida
- Honorable Mention: team **Insecurity**, the University of Florida

Hack ML

The new Hack ML (machine learning) competition, the first of its kind, challenged contestants to fortify notoriously fragile deep learning–based artificial intelligence. In preliminary rounds, teams from all over the world were invited to submit compromised neural network models. The competition leaders anonymized, and then redistributed them so that competitors could devise techniques for reverse-engineering and healing the compromised models. The best attackers and defenders proceeded to the finals to demonstrate their novel tactics during the final round. One element of the challenge — developing new strong backdoor attacks on facial recognition models — required teams to train the neural networks to misidentify human faces when a physical prop — a "trigger" — was held near them during staged photoshoots at CSAW at NYU Tandon.

- Top Defense Team Award: team **DukeCEI,** Duke University
- Top Attack Team Award: team **SiceML**, the University of Pittsburgh, Georgia Institute of Technology, Carnegie Mellon University, and Pennsylvania State University

Hack3D

In an event focused on anti-counterfeiting methods in 3D printing, competitors were first tested in reverse engineering a 3D CAD model, then, during the final round, teams tried to print 3D parts embedded with anti-counterfeiting features.

- First place: team **SNEKSAD**, NYU Abu Dhabi
- Second place: team **pwndevils**, Arizona State University
- Third place: team **AGGIES**, Texas A&M University

Logic Locking Conquest

In this new contest, students were challenged to solve the problem of securing chips during the manufacturing process, a fact-moving area of research. Often before sending their chip designs to a foundry, designers "lock" their designs, a process involving modifying the original digital circuit in such a way that the correct functionality can be unlocked only with a specific key, or a correct sequence of keys. Doing so prevents potential bad actors in the supply chain (including a foundry) from changing the design by inserting back doors that could allow future attacks or stealing intellectual property. During the preliminary round, teams worked on a chip design devised by students and mentors at NYU Abu Dhabi and the University of Florida to either find the key or devise a new one in order to protect the circuitry. The best solutions advanced to the finals, where seven teams competed in Brooklyn, including two from India, who competed remotely.

- First place: team **CMU**, Carnegie Mellon University
- Second place: team **NuLogiCS**, Northwestern University
- Third place: team **IO**, the University of California San Diego

Policy Competition

This competition — at NYU Tandon and the Indian Institute of Technology, Kanpur, India (IIT Kanpur) — attracts students who are interested in the nexus of law, policy, and emerging security issues. The competition challenges interdisciplinary teams to develop proposals for impactful cybersecurity public policy. The number of teams more than doubled since last year, attracting proposals from a dozen universities. Winners at the NYU Tandon finals were **Wesleyan University**, which won first place, and two different teams from the **United States Naval Academy**, taking second and third place.

Applied Research

This competition, held at NYU Tandon, Grenoble-INP Esisar, IIT Kanpur, NYU Abu Dhabi, and Ben-Gurion University, accepts only peer-reviewed security papers that have already been published by scholarly journals and conferences. One of the student authors of each paper present in poster format to judges.

- First place: Emma Dauterman of **Stanford University** presented for authors of "True2F: Backdoor-resistant authentication tokens"
- Second place: Hadi Abdullah presented for the **University of Florida** authors of "Practical Hidden Voice Attacks against Speech and Speaker Recognition Systems"

- Third place: Xianghang Mi of **Indiana University Bloomington** presented for the authors of "Dangerous Skills: Understanding and Mitigating Security Risks of Voice-Controlled Third-Party Functions on Virtual Personal Assistant Systems"

Security Quiz Bowl

Thirty teams competed during CSAW finals at NYU Tandon in the fast-paced game show sponsored by IBM. Students were quizzed on hardware, malware, software tools, reverse engineering, languages, culture, forensics, file systems, protocols, software, and more.

- First place: team **perfect blue**, a mixed team from the University of Waterloo, Purdue University, Drexel University, and the Georgia Institute of Technology
- Second place: team **PPP,** Carnegie Mellon University
- Third place: team **G8rs**, University of Florida

Closing keynote speakers from DTCC outlined the massive business impact of security in the financial services industry. Sandeep Singh, DTCC executive director-digital marketplace and API strategy, and Christopher Walsh, DTCC executive director of risk analytics, announced a year-long contest on AI security in a microservices application for CSAW 2020, with details to be released in early 2020.

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.

More than 250 students from across Europe, India, Israel, Mexico, and North Africa scored wins to take them to academic hubs to compete in CSAW finals at the same time that NYU Tandon was hosting the best students from Canada and the United States. The 2019 CSAW finals were held November 6–8 at:

- NYU Tandon in Downtown Brooklyn, New York
- IIT Kanpur
- Grenoble-INP Esisar in Valence, France
- Ben-Gurion University of the Negev and the University of Haifa in Israel (with IBM Research-Haifa and the IBM Cyber Security Center of Excellence)
- Universidad Iberoamericana (Ibero) in Mexico City
- NYU Abu Dhabi in the United Arab Emirates

The full list of international winners and information will be posted at csaw.engineering.nyu.edu.

Follow@CSAW_NYUTandon and join the conversation at #CSAW2019.

CSAW U.S.- Canada Sponsors are: Gold Level – Army Research Office, Capsule8, DTCC, National Science Foundation; Silver Level – BAE Systems, IBM, Red Balloon Security; Bronze Level – ConEdison, Facebook, Flatiron Health, Jefferies, JPMorgan Chase & Co., RiskEcon Lab for Decision Metrics @

Courant Institute of Mathematical Sciences, T. Rowe Price; Supporting Level — Bank of America; CMU Information Networking Institute; Contributing Level – Aflac, Applied Computer Security Associates, CTFd, Datadog, TIAA, Raytheon, Uber, Vector35.

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.

About the NYU Center for Cyber Security
The NYU Center for Cybersecurity (CCS) is an interdisciplinary research institute dedicated to training the current and future generations of cybersecurity professionals and to shaping the public discourse and policy, legal, and technological landscape on issues of cybersecurity. NYU CCS is a collaboration between NYU School of Law, NYU Tandon School of Engineering, and other NYU schools and departments. For more information, visit cyber.nyu.edu.

###