Note: Images available at
https://nyutandon.photoshelter.com/galleries/C0000ieY7SWamx1Q/G0000.bqo7H9xLhA/CSAW-2018-Release

Immediate Release

World's Biggest Student-Led Cybersecurity Games

Announce Winners of CSAW 2018

**NYU Tandon School of Engineering Turned Brooklyn into Epicenter of
North America's Top Young Hackers and Protectors, While Finalists across Globe Competed
Simultaneously in France, India, Israel, Mexico, and North Africa**

BROOKLYN, New York, Tuesday, November 13, 2018 — The 15th anniversary edition of the world's largest student-led hacking and protection competitions, CSAW, closed Saturday at universities across four continents with record-breaking participation in the face of reports of shortfalls of up to 3 million experts globally.

The founder of CSAW, the New York University Tandon School of Engineering, welcomed 130 student finalists in seven separate competitions, and another 267 competed in the final rounds hosted by schools in France, India, Israel, and Mexico. In Brooklyn alone, some 100 professionals and faculty worked with NYU Tandon student leaders to create, judge, and organize the giant event, supported by 30 industry and government partners. The Borough President proclaimed November 8 as NYU Tandon CSAW 15th Anniversary Day in Brooklyn.

To earn spots in the coveted final rounds, this year's contestants bested nearly 20,000 competitors worldwide. Since its inception, nearly 150,000 people have competed in CSAW preliminary challenges.

At the finals for the United States and Canada, held in Brooklyn, students won cash prizes, more than $1 million in scholarships to NYU Tandon, and "medals" designed and printed in the NYU MakerSpace – the exact place in which the students competed November 8-10, 2018.

-more-

Students participated in a career fair and networking events designed to introduce them to mentors and peers who can form strong networks for their later careers. Alumni who ran the first CSAWs and went on to work in prestigious positions and to found security companies offered career insight (and a few confessions) during a panel discussion in an auditorium packed with the most accomplished young hackers and protectors in the two countries. Industry experts and judges were able to engage in professional develop opportunities via the Frontiers of Cyber Security Workshop, which focused on security analytics and secure deployment of machine learning, and a Friday luncheon hosted by Bank of America.

"CSAW exemplifies the hope that engineering brings to a world grappling with massive technological change," said NYU Tandon Dean Jelena Kovačević. "Every one of the 400 finalists earned this elite status through creativity, curiosity, and dedication. They are destined to be leaders who will protect our society and economy. Our congratulations go out to them and to the faculty and parents who encouraged and helped educate them."

She added: "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."

Among the NYU Tandon CSAW winners were many repeat winners and some surprises, too.

Capture the Flag and Security Quiz Bowl

The flagship event of CSAW, Capture the Flag (CTF), once again tested the hacking and protecting skills of undergraduate teams. The notoriously difficult final round — completed by none of the teams this year — demanded a profound understanding of the roles and ramifications of cybersecurity and covered pwning, reverse engineering, web, cryptography, and forensics.

Included among the challenges was a video game developed by Vector35, called PwnAdventure Sourcery, in the style of a Super Nintendo game. CTF competitors hacked it using elements built into the game. Players cast "spells" using actual computer code and interacted with virtual devices that ran their own code in the game world.

For the second year in a row, a team from **Rensselaer Polytechnic Institute** took home **top honors**. The RPISEC team pulled out the win in the final minutes of the 36-straight-hour competition by solving a final challenge. Two team members — Jack Dates and Josh Ferrell — returned from last year's winning team. They were joined by Aidan Noll and Jack Phillips.

Carnegie Mellon's PPP team took second place: Valerie Choung, Sam Damashek, Kevin Geng, and Samuel Kim represented the team that has been a podium winner annually since the early years of CSAW.

In third place was the all-freshmen Perfect Blue team: Alex Lin of **Purdue University,** Sampriti Panda of **Drexel University,** Kevin Shen of **University of Maryland,** and Stephen Tong of **Georgia Institute of Technology.**

Immediately after the grueling 36-hour CTF competition, Perfect Blue and RPISEC took the stage to compete in the **Security Quiz Bowl**, a fast-paced and difficult game show-like competition covering

technology, current events, and history, hosted by gold sponsor, Capsule8. These teams placed second and third, respectively.

Taking first place in the Security Quiz Bowl was the University of Maryland Baltimore County Cyber Dawgs — who similarly showed few signs of exhaustion after the marathon CTF: Joe Aurelio, Seamus Burke, Zack Orndorff, and Grant Spencer. The school also took honors in the Embedded Security Challenge.

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

Applied Research Competition

Long recognized as the premier showcase for young security researchers whose work has already appeared in peer-reviewed scientific journals and conferences, the Applied Research Competition requires a poster and one student to present the research to a panel of judges.

First place: University of Tennessee, Knoxville Jared Smith and Max Schuchard; the former presented their paper, "Routing Around Congestion: Defeating DDoS Attacks and Adverse Network Conditions via Reactive BGP Routing."

Second place: Kexin Pei of **Columbia University**, Yinzhi Cao of **Johns Hopkins University,** Junfeng Yang and Suman Jana, **both of Columbia University;** Pei presented the paper "DeepXplore: Automated Whitebox Testing of Deep Learning Systems." Jana was a co-author of the third-place paper, as well.

Third place: Shankara Pailoor of the **University of Texas at Austin,** Andrew Aday and Suman Jana, both of **Columbia University;** Pailoor presented the paper "MoonShine: Optimizing OS Fuzzer Seed Selection with Trace Distillation."

Embedded Security Challenge

This challenge took a red team/blue team approach, in which security experts from NYU Tandon competed with participating university teams to mimic the real-world attacks and defenses of the connected devices that comprise the Internet of Things. Teams were challenged to exploit weaknesses of smart light bulbs to exfiltrate data in a nearby network that should have been air gapped — not connected to the Internet. This particularly difficult challenge was led by NYU Abu Dhabi Modern Microprocessors Architecture Lab (MoMA) and the U.S. Office of Naval Research.

First place: University of Delaware team Blue Hens: Patrick Cronin, Charles Gouert, and Fateme Hosseini with faculty advisors Chengmo Yang and Nektarios Tsoutsos. Cronin, Hosseini, and Yang won second place in last year's Embedded Security Challenge.

Second place: University of Maryland Baltimore County team UMBC Secrets Lab: Md Toufiq Hasan Anik, Hasib-Al-Rashid, and Trevor Kroeger, with faculty advisor Naghmeh Karimi

Third place: Texas A&M University team Texas A&M Hardware Defense: Michael Hall, Mahesh Naidu, Ryan Vrecenar, and Josh Zschiesche with faculty advisors Stavros Kalafatis and Jeyavijayan Rajendran

Both Tsoutsos and Rajendran are alumni of NYU's noted hardware security research team and former student team leads for the Embedded Security Challenge.

Hack3D Competition

New this year was a test in an emerging area of cybersecurity: protecting the additive manufacturing process now employed to produce high-value components used in aerospace, automotive, medical devices, and more. In the final round, competitors were challenged to thwart cutting-edge anti-counterfeiting measures developed by NYU researchers to 3D print a part with high quality. As with the Embedded Security Challenge, knowledge gained in this competition will inform future research in the new field, including the pioneering work being conducted at NYU Tandon.

First place: NYU Abu Dhabi team A5-015: Nishant Suresh Aswani and Barkin Simsek

Second place: NYU Tandon team NotStrong: Songyu Du and Aiqi (Angela) Zhou

Third place: NYU Abu Dhabi team StreetCats: Qutaiba Al-Nuaimy and Shunsuke Kasahara.

Policy Competition

Student teams presented proposals for major policy changes in cybersecurity and privacy affecting society, government, and law. The Policy Case Competition joined NYU Tandon for the first time in organizing this multidisciplinary challenge.

First place: Brown University: Adam DiPetrillo, George "Donnie" Hasseltine, Joshua Snavely, and Chad Thiemann. Their policy memo provided recommendations for protecting and securing the U.S. electoral systems through data security and breach prevention. They recommend to the United States Committee on Homeland Security that voter and election data should be managed and encrypted in compliance with the National Institute of Standards and Technology Cybersecurity Framework and related Department of Homeland Security (DHS) infrastructure cybersecurity measures.

Second place: United States Naval Academy: Kameron Chumley, Cameron Cook, and Brendan Reilly. An annual podium finisher since the launch of the Policy Competition in 2014, the Naval Academy won the competition last year. This year's policy memo recommended establishing honeypots (sites set up to gather intelligence) via the FBI's Cyber Division. These would augment DHS's Automated Indicator Sharing (AIS) program and provide the private sector with valuable information to establish security defense measures.

Third place: United States Military Academy: Liam Furey, Peter Kim, Robert Norwood, and Amanda Roper. They outlined steps DHS can take to improve the overall security of the digital infrastructure, including expanding and focusing the existing AIS system, establishing a Cyber Threat Intelligence Center to analyze and publish the data collected by AIS, and marketing these two systems as a must-have solution to both private- and public-sector entities.

Red Team Competition

High school teams used their skills of forensics, cryptography, reverse engineering, and exploitation to infiltrate and analyze a fictional company, Quentrian. They had to gain a back door to its server login, printers, emails, payroll, bank balances, and more to learn as much about the company as they could, including its products, an illicit side business (someone in the company was selling user data), names of Quentrian executives, the thief who was selling user data, and the murder victim. Teams were ranked on how much they learned.

First place: Dos Pueblos High School of Goleta, California, team 1064CBread: Paul Grosen, Blake Lazarine, and Nathan Wachholz. This was the fourth consecutive CSAW for Grosen, and the second consecutive for Wachholz.

Second place: Montgomery Blair High School, Rockville, Maryland, team n0de: Kevin Higgs, Ian Rackow, and William Wang. Rackow and Wang were part of the team n0de that won third place last year, when another team from the same school won first place. Montgomery Blair High School has become a regular fixture at the CSAW finals.

Third place: West Windsor-Plainsboro High School North, Plainsboro, New Jersey, team let_down: Spencer Hua, Parth Shastri, and Daniel Wang

Cyber Journalism Award

The only CSAW contest for non-students recognizes excellence in reporting on cybersecurity and privacy. Judges chose **Jen Wieczner as winner of the 2018 CSAW Cyber Journalism Award** for The Surprising Redemption of Bitcoin's Biggest Villain, which delves into Mt. Gox Chief Executive Mark Karpelès' attempts to recover lost funds and exonerate himself of a multimillion-dollar theft in which he was a prime suspect. Wieczner is a senior writer at *Fortune* and co-founding editor of *The Ledger,* Fortune's financial technology and blockchain publication.

The competition is a joint project of the NYU Tandon School of Engineering and the NYU Arthur L. Carter Journalism Institute.

About CSAW

The CSAW games, founded as a small contest called Cyber Security Awareness Week by and for NYU Tandon students studying under Professor Nasir Memon, 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. NYU Tandon's student-led Offensive Security, Incident Response and Internet Security (OSIRIS) laboratory, 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 where they competed in CSAW finals at the same time that NYU Tandon was hosting the best students from Canada and the United States:

- Indian Institute of Technology, Kanpur (IIT Kanpur)
- Grenoble-INP Esisar in Valence, France

- Ben-Gurion University 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

For a full list of international winners and information on the challenges, visit csaw.engineering.nyu.edu. Follow @CSAW_NYUTandon and join the conversation at #CSAW2018.

Many of the sponsors from the United States and Canada worked with NYU students to develop the challenges, acted as judges and mentors, and recruited at the popular career fair:
Gold Level — Capsule8, IBM, the United States Navy Office of Naval Research
Silver Level — BAE Systems, Bank of America, T. Rowe Price
Bronze Level — Estée Lauder Companies, Facebook, Flatiron Health, Jane Street, Jefferies, JPMorgan Chase & Co., Palo Alto Networks, Raytheon, Red Balloon Security, Synopsys, TD Bank, Uber
Supporting Level — Cisco Tetration Analytics, Cubic Corporation, NCC Group, Qrypt
Contributing Sponsors: Applied Computer Security Associates, CTFd, Datadog, Include Security, Ret2 Systems, RiskEcon Lab @Courant Institute of Mathematical Sciences, Splunk, and 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.

###