There was much that was new about CSAW’22, held November 9-12 at several sites around the world. For instance, it featured the debut of three new competitions (though one did not receive enough entries to make it to the finish line), and the US-Canada site saw events relocated to the actual Tandon “headquarters” of the Center for Cybersecurity at 370 Jay Street. Yet, in many ways the event felt more like a comfortable return to familiar territory than an exploration of a new frontier. The switch back from the Gather virtual platform used the past two years to Brooklyn (or Abu Dhabi or Valence for attendees at the CSAW MENA and Europe sites), meant that, once again, attendees had opportunities for the informal networking and socializing that had previously been a hallmark of the program.

In addition to Tandon’s Brooklyn location, CSAW’22 was held, either in-person or virtually, at four other sites in Europe (Grenoble INP - Esisar in Valence, France), Middle East/North Africa (NYU Abu Dhabi, United Arab Emirates), India (Indian Institute of Technology in Kanpur), and Mexico (Universidad Iberoamericana in Mexico City). By the numbers, this 19th edition of “the world’s most comprehensive student-run cybersecurity event,” boasted:

- **3,142** Total Participants (including those involved in qualifying rounds)
- **1,420** Qualifying Teams
- **128** Team Finalists
- **9** Sponsors
- **16** Partner Organizations
- **7** Competitions

Yet, the numbers do not tell the whole story. Over the next few pages, we present highlights from the event in text and photos. We’ll also share some “backstage insights” from two of the new competitions, Hack My Robot, which debuted at NYU Abu Dhabi, and AI vs. Humans, which debuted in Brooklyn.

Lastly, we’ll also share a comprehensive list of all the first place winners of this year’s competitions.

As CSAW has evolved into a global network of events, it has benefited from the input and support of a number of partner organizations. These partners develop problems and scenarios for individual competitions, see that competitors receive the necessary information and materials, and recruit judges. The NYU Center for Cybersecurity thanks its 2022 partners: NYU OSIRIS Lab, the NYU Center for Global Affairs, NYU Cyber Fellows, the NYU Wasserman Center for Career Development, NYU Tandon Career Hub, the Interdisciplinary Centre for Cyber Security and Cyber Defense of Critical Infrastructures at IIT Kanpur, the NYU Abu Dhabi Center for Cyber Security, the University of Delaware College of Engineering, Grenoble Alpes Cybersecurity Institute, Valencia Research Laboratory, Grenoble INP Institut d’ingénierie et de management, Modern Microprocessors Architecture Lab at NYU Abu Dhabi, Global CyberPeace Challenge, and CTFd. Corporate and government sponsors for CSAW'22 US-Canada were Siemens, DTCC, Zellic.io, Con Edison, Meta, Trail of Bits, Carnegie Mellon University Information Networking Institute, New York State Empire State Development, and the National Science Foundation.

**CSAW'22 WRAP-UP:**

**THERE’S NO PLACE LIKE HOME**

There was much that was new about CSAW’22, held November 9-12 at several sites around the world. For instance, it featured the debut of three new competitions (though one did not receive enough entries to make it to the finish line), and the US-Canada site saw events relocated to the actual Tandon “headquarters” of the Center for Cybersecurity at 370 Jay Street. Yet, in many ways the event felt more like a comfortable return to familiar territory than an exploration of a new frontier. The switch back from the Gather virtual platform used the past two years to Brooklyn (or Abu Dhabi or Valence for attendees at the CSAW MENA and Europe sites), meant that, once again, attendees had opportunities for the informal networking and socializing that had previously been a hallmark of the program.

In addition to Tandon’s Brooklyn location, CSAW’22 was held, either in-person or virtually, at four other sites in Europe (Grenoble INP - Esisar in Valence, France), Middle East/North Africa (NYU Abu Dhabi, United Arab Emirates), India (Indian Institute of Technology in Kanpur), and Mexico (Universidad Iberoamericana in Mexico City). By the numbers, this 19th edition of “the world’s most comprehensive student-run cybersecurity event,” boasted:

- **3,142** Total Participants (including those involved in qualifying rounds)
- **1,420** Qualifying Teams
- **128** Team Finalists
- **9** Sponsors
- **16** Partner Organizations
- **7** Competitions

Yet, the numbers do not tell the whole story. Over the next few pages, we present highlights from the event in text and photos. We’ll also share some “backstage insights” from two of the new competitions, Hack My Robot, which debuted at NYU Abu Dhabi, and AI vs. Humans, which debuted in Brooklyn.

Lastly, we’ll also share a comprehensive list of all the first place winners of this year’s competitions.

As CSAW has evolved into a global network of events, it has benefited from the input and support of a number of partner organizations. These partners develop problems and scenarios for individual competitions, see that competitors receive the necessary information and materials, and recruit judges. The NYU Center for Cybersecurity thanks its 2022 partners: NYU OSIRIS Lab, the NYU Center for Global Affairs, NYU Cyber Fellows, the NYU Wasserman Center for Career Development, NYU Tandon Career Hub, the Interdisciplinary Centre for Cyber Security and Cyber Defense of Critical Infrastructures at IIT Kanpur, the NYU Abu Dhabi Center for Cyber Security, the University of Delaware College of Engineering, Grenoble Alpes Cybersecurity Institute, Valencia Research Laboratory, Grenoble INP Institut d’ingénierie et de management, Modern Microprocessors Architecture Lab at NYU Abu Dhabi, Global CyberPeace Challenge, and CTFd. Corporate and government sponsors for CSAW'22 US-Canada were Siemens, DTCC, Zellic.io, Con Edison, Meta, Trail of Bits, Carnegie Mellon University Information Networking Institute, New York State Empire State Development, and the National Science Foundation.

**CSAW'22 WRAP-UP:**

**THERE’S NO PLACE LIKE HOME**

There was much that was new about CSAW’22, held November 9-12 at several sites around the world. For instance, it featured the debut of three new competitions (though one did not receive enough entries to make it to the finish line), and the US-Canada site saw events relocated to the actual Tandon “headquarters” of the Center for Cybersecurity at 370 Jay Street. Yet, in many ways the event felt more like a comfortable return to familiar territory than an exploration of a new frontier. The switch back from the Gather virtual platform used the past two years to Brooklyn (or Abu Dhabi or Valence for attendees at the CSAW MENA and Europe sites), meant that, once again, attendees had opportunities for the informal networking and socializing that had previously been a hallmark of the program.

In addition to Tandon’s Brooklyn location, CSAW’22 was held, either in-person or virtually, at four other sites in Europe (Grenoble INP - Esisar in Valence, France), Middle East/North Africa (NYU Abu Dhabi, United Arab Emirates), India (Indian Institute of Technology in Kanpur), and Mexico (Universidad Iberoamericana in Mexico City). By the numbers, this 19th edition of “the world’s most comprehensive student-run cybersecurity event,” boasted:

- **3,142** Total Participants (including those involved in qualifying rounds)
- **1,420** Qualifying Teams
- **128** Team Finalists
- **9** Sponsors
- **16** Partner Organizations
- **7** Competitions

Yet, the numbers do not tell the whole story. Over the next few pages, we present highlights from the event in text and photos. We’ll also share some “backstage insights” from two of the new competitions, Hack My Robot, which debuted at NYU Abu Dhabi, and AI vs. Humans, which debuted in Brooklyn.

Lastly, we’ll also share a comprehensive list of all the first place winners of this year’s competitions.

As CSAW has evolved into a global network of events, it has benefited from the input and support of a number of partner organizations. These partners develop problems and scenarios for individual competitions, see that competitors receive the necessary information and materials, and recruit judges. The NYU Center for Cybersecurity thanks its 2022 partners: NYU OSIRIS Lab, the NYU Center for Global Affairs, NYU Cyber Fellows, the NYU Wasserman Center for Career Development, NYU Tandon Career Hub, the Interdisciplinary Centre for Cyber Security and Cyber Defense of Critical Infrastructures at IIT Kanpur, the NYU Abu Dhabi Center for Cyber Security, the University of Delaware College of Engineering, Grenoble Alpes Cybersecurity Institute, Valencia Research Laboratory, Grenoble INP Institut d’ingénierie et de management, Modern Microprocessors Architecture Lab at NYU Abu Dhabi, Global CyberPeace Challenge, and CTFd. Corporate and government sponsors for CSAW'22 US-Canada were Siemens, DTCC, Zellic.io, Con Edison, Meta, Trail of Bits, Carnegie Mellon University Information Networking Institute, New York State Empire State Development, and the National Science Foundation.
THE VIEW FROM THE 10TH FLOOR: CSAW’22 IN BROOKLYN

At the US-Canada site in Brooklyn, CSAW started with a welcoming dinner on Wednesday evening, November 9, and concluded with an awards ceremony on Saturday morning, November 12. In-between attendees got to hear talks by cybersecurity professionals, chat with representatives from industry, academia, and open source companies about career opportunities, and perhaps most importantly, meet other students who share an interest in solving tomorrow’s cybersecurity issues.

As always, the heart of the event was its competitions, and attendees at the Brooklyn site got to compete in or observe the finals of seven, the most held at any single site. Finalist presentations in the Hack3D competition filled the better part of Thursday, November 10, while the 36 hour Capture the Flag competition and the Policy Competition both got underway later that day. The Policy Competition, which is organized by students from NYU’s Center for Global Affairs, Tandon School of Engineering, College of Arts and Sciences, Graduate School of Arts and Sciences, Robert F. Wagner Graduate School of Public Service and the Law School, was one of several competitions that remained online in order to incorporate participants from across several meeting sites within the same session. U.S. participants in this year’s competition were asked to propose solutions to national security concerns stemming from the integration of “smart” technology connected across communities, while presentations of their counterparts from other parts of the world revolved around the current US-China technology competition for the global “smart” technology market.

Like the policy competition, the Hack3D competition was run as just one global event. Several of the teams included one or more participants from other CSAW sites, and so the finals were done hybrid, with several teams competing remotely. The balance of the competitions, including the Embedded Security Challenge (which marked its 15th anniversary in 2022), Applied Research, Logic Locking, and the brand new AI vs. Humans competition (see article on page 16) were held onsite on Friday.
Rounding out the list of speakers were Kurt Rosenfeld, a software engineer who develops distributed systems at Google, and Dr. Hammond Pearce, a research assistant professor at the NYU Center for Cybersecurity. Rosenfeld spoke about the role of time servers and how the failure of these devices can lead to a series of negative consequences. To protect these devices he recommended avoiding semantics that cannot express uncertainty (that is, the machine should be able to say “I don’t know” if it doesn’t have access to a secure source of time), and using multiple servers to reduce the impact if one server in the system lies. Lastly, Dr. Pearce shared some insights from a study he conducted with other Tandon faculty on possible vulnerabilities generated through the use of GitHub Copilot.

Many of the speakers stayed on in the afternoon to represent their companies at a Career Fair. Other institutions participating in the fair were Trail of Bits and the Carnegie Mellon Information Networking Institute.
NEW COMPETITIONS REFLECT THE GROWING SCOPE OF CYBER THREAT TOPICS

The introduction of new CSAW competitions can be seen as something of a barometer indicating the emergence of either a new type of attack or a new threat target. The events making their debut this year, Hack My Robot and AI vs. Humans, are no exceptions to this rule. The former acknowledges the cybersecurity needs of “increasingly digitalized construction environments,” while the latter recognizes that even hardware security tools built with the aid of artificial intelligence are not invulnerable.

Hack My Robot, staged exclusively at the NYU Abu Dhabi campus in the CSAW MENA region, asked student teams to gather and evaluate data collected from a fully functional construction progress monitoring robot, identify potential ways to compromise the system, and recommend improvements that could secure the site in question. The brand new event was open to both undergraduate and graduate students enrolled in any university within the region and attracted 19 students from three different schools.

According to Semih Sonkor, the lead organizer for Hack My Robot, the competition reflects the goals of the NYU Abu Dhabi-based S.M.A.R.T. Construction Research Group, where Sonkor serves as a research assistant. Under the direction of Dr. Borja García de Soto, assistant professor of civil and urban engineering, the group researches the challenges of an increasingly automated and technology- dependent field (the “ART” of the group’s name stands for Artificial intelligence, Robotic systems and automation, and Technology integration and information modeling). As such, recruiting participants for the inaugural run of the competition meant “actively reaching out to all engineering disciplines including computer, electrical, mechanical, and civil engineering,” Sonkor reported.

Taking us through the stages of the competition, Sonkor explained that, in the initial round students “answered open-ended questions to present their ideas on how to hack the given robotic system.” He noted that in this opening round, the judges were looking for responses that were “feasible/achievable, relevant to the context of the competition” and showed enough technical knowledge in cybersecurity and robotics “to prove eligibility for the final round.” For the final round, the criteria included “the teams’ ability to alter/modify the data collected by the robot, or alter the predefined functionalities of the robotic system.” In both rounds, he emphasized, “creativity and out-of-the-box thinking were also crucial.”

In the latter category, the participants did not disappoint. Sonkor observed that, “all the teams came out with very different approaches and innovative ideas during the challenge.” When asked for a specific example of such an innovation, he points to one entry that “created multiple fictitious networks so that if the other teams wanted to attack their network, they wouldn’t know which network was the real one. The judges found that particularly interesting.”

Team SENTRY of King Abdullah University of Science and Technology in Saudi Arabia took the inaugural first place award, but, as Sonkor points out, all finalists can be said to be winners, if they “learned new techniques and added to their existing cybersecurity knowledge.” He adds that “being strategic about time was crucial in the final round. We hope that they understood the importance of not getting stuck and insisting on any step and moving forward with the other ones to achieve the maximum possible score.”

Those in the MENA region that did not get a chance to compete this year will have such an opportunity in the years ahead. Sonkor reported that the organizers, which included Dr. Garcia de Soto, Dr. Samuel Prieto Ayllón, a postdoctoral associate at NYUAD, Xinghui Xu, a PhD candidate and research assistant at NYUAD, and Dr. Farshad Khorrami, a professor of electronic and computer engineering at NYU Tandon, are planning to make Hack My Robot an annual event. In organizing for future competitions, Sonkor stated that “having diversity in terms of schools and countries within the MENA region will be one of our priorities,” as well ensuring that all criteria are “manageable yet challenging for the participant teams.”

Organizers of the Hack My Robot Competition (from l to r) Borja García de Soto, Samuel A. Prieto Ayllón, Semih Sonkor, and Xinghui Xu.
HONORING THE BEST OF CSAW’22

As CSAW is a global event, we decided to make our list of first place winners as comprehensive as possible. That is, we are publishing here a master list of all of the year’s first place winners, no matter where they competed. To see a list of all the finalists in any particular competition, go to the CSAW website (https://www.csaw.io/) and click on the appropriate links.

AI VS. HUMANS

• US-Canada | Team CCNY, City College of New York
  Vedika Saravanan, Mohammad Walid M Charrwi, Facundo Aguirre
  Advisor: Prof. Samah Saeed

APPLIED RESEARCH COMPETITION

• Europe | Sinem Sav, Swiss Federal Institute of Technology Lausanne (Switzerland), presenting POSEiDON: Privacy-Preserving Federated Neural Network Learning

• MENA | Naif Mehanna, Inria Centre, University of Lille (France), presenting DRAWNAPART: A Device Identification Technique Based on Remote GPU Fingerprinting

• US-Canada | Reethika Ramesh, University of Michigan, Ann Arbor (US) presenting VPNalyzer: Systematic Investigation of the VPN Ecosystem

CAPTURE THE FLAG

• Global and US-Canada | Perfect Blue
  Alex Lin - Stanford University; Jazzy Bedi and Larry Yuan - University of Waterloo; Sam Schweigel - University of British Columbia

• Europe | Tower of Hanoi, Politecnico di Milano (Italy)
  Marco Meinardi, Gabriele Digregorio, Daniele Mammine, Davide Luca Merli

• India | docker-chan’s simps, IIT Roorkee
  Priyansh Rathi, Kartikey Kumar, Manas Ghandat, Gyanendra Kumar Banjare

PLAYING CAT AND MOUSE WITH AI TOOLS

The other new competition debuted in Brooklyn but was developed at Texas A&M University by graduate research assistant Vasudev Gohil and Tandon Ph.D. alumnus Dr. Satwik Patnaik, now a post-doctoral researcher at Texas A&M. AI vs. Humans invited participants to step into the shoes of either an attacker or a defender looking to exploit or protect against vulnerabilities in state-of-the-art AI-based detection tools.

The origins of the competition, as explained recently by Dr. Patnaik, was to take advantage of crowdsourcing, which he dubbed “a powerful tool in hardware security competitions, allowing for a wide range of expertise and perspectives to contribute to the identification and remediation of security vulnerabilities.” A total of 49 participants registered for the initial round, representing 16 universities, along with a few representatives from industry.

The official description of the competition on the CSAW website notes that it is “designed to mimic real-world scenarios where an attacker can inject Trojans to cause damaging consequences ranging from altering the chip's functionality and leaking sensitive data, such as cryptographic keys, to causing denial-of-service attacks.” Competitors were “provided small-sized designs to implement/test their techniques, inspect the performance by interacting with AI-based tools, and subsequently improve scalability for large-sized designs.” The final submission was a written report detailing the methodology used by the teams that highlighted how they evaded the AI-based defense tool.

Interestingly enough, though competitors were free to act as attackers or defenders, Gohil noted that no submissions were received for the defender's role, a somewhat surprising outcome because “a lot of the coding would be common.” He also observed that, during the competition, one of the teams discovered an improvement to an existing Trojan detection technique and is continuing to develop the method.

Similar to the organizers of Hack my Robot, Dr. Patnaik reports that there are plans to continue the AI vs. Humans competition, though they might explore the feasibility of using another hardware security problem(s). As for the takeaway from this year’s event, he notes, “we hope that the competitors realize that detecting Trojans is a difficult task” and that “researchers continue to develop stronger and scalable methods to detect hardware Trojans that conform to realistic assumptions.”

In addition to Gohil and Dr. Patnaik, the organizers of AI vs. Humans, all from Texas A&M, were: Hao Guo, a Master’s student working at the Texas A&M Secure and Trustworthy Hardware Lab, and Dr. Jeyavijayan (JV) Rajendran, Assistant Professor, Electrical & Computer Engineering.
• MENA | ShellSec, Ecole Nationale Supérieure d’Informatique (Algeria)
  Oussama Abdallah Merouan, Hithem Lamri, Mohamed Laid Malik Mabrouki, Mohamed Amokrane Abdelmalek

• Mexico | PumaHat, Universidad Nacional Autónoma de México-Facultad de Ingeniería
  Hector Espino Rojas, Pablo Martínez Ramírez, Rodrigo Zacatelco Zenteno
  Embedded Security Challenge

EMBEDDED SECURITY CHALLENGE

• Europe | USCT, University of Piraeus (Greece)
  Konstantinos Spyridon Mokos, Filippos Fotopoulos, Ilias Fiotakis, Iasonas Konstantinos Manthos, Athanasios Papadimitriou

• India | SEAL IITKGP, IIT Kharagpur
  Kuheli Pratihar, Nimitish Mishra, Shubhi Shukla, Anirban Chakraborty, Debdeep Mukhopadhyay

• US-Canada | The Quad,
  University of Calgary (Canada)
  Joey Ah-kiow, Abdelrahman Elnaggar, Anudeep Dharavathu, Subroto Nath, Dillon Sahadevan, Benjamin Tan

HACK3D

• Global | Roar, Clemson University (US)
  Ethan Wescoat, Flanagan Waldherr, Shamanth Manjunath

HACK MY ROBOT

• MENA | Team SENTRY, King Abdullah University of Science and Technology (Saudi Arabia)
  Ioannis Zografopoulos, Alyah Alfageh, Li Zhou, Shijie Pan
  Logic Locking Conquest

• Global | Fancy Logiciers (US)
  Michael Dominguez, California State University Long Beach
  Yeganeh Aghamohammadi, University of California Santa Barbara

POLICY COMPETITION

• Global | Team 7: National Security Concerns,
  United States Military Academy, West Point (USA)
  Nicholas Liebers, Alex Strawley, Vishnu Kumar, Nathan Seybert