NYU TANDON SCHOOL OF ENGINEERING

NYU Center for Cybersecurity

CYBER BYTE

SPRING 2020

HOW TO CELEBRATE CSAW'S SWEET 16:

6 GLOBAL SITES + 9 COMPETITIONS +167 FINALISTS

For three days in November, NYU Tandon School of Engineering was a proud host of the 16th edition of Cyber Security Awareness Worldwide or CSAW. The Brooklyn campus of Tandon, the host site for the event for the United States and Canada, was one of six locations around the world to host two or more CSAW competitions from November 6-8, 2019.

Though it is the world's most comprehensive student-led cybersecurity competition, numbers by themselves, can not tell the whole story of any CSAW gathering. But, a few figures from the 2019 edition do indicate how the competition has grown since 2003.

- Total number of teams that participated in qualification rounds: 1225, drawn from 90 countries.
- Total number of finalist teams across all regions: 167
- Total number of finalist teams at Tandon: 72 teams, comprising 164 students.
- Approximate number of attendees at Brooklyn events: 640
- Total number of sponsoring companies: 24

The U.S./Canada site added two new competitions, bringing the total number held in Brooklyn to nine. The newest competitions— Hack ML, in which students had to train neural networks to intentionally thwart facial recognition software, and Logic Locking, in which competitors attempted to hack chips digitally locked by their designers—were added this year because the technologies involved have become desirable attack surfaces, requiring innovative solutions. As Ramesh Karri, co-chair of the Center for Cybersecurity (CCS) observed, "By adding these contests, CCS events generate new avenues of research."

IN THIS ISSUE

Student Competitors @ CSAW

(Continued from page 1)

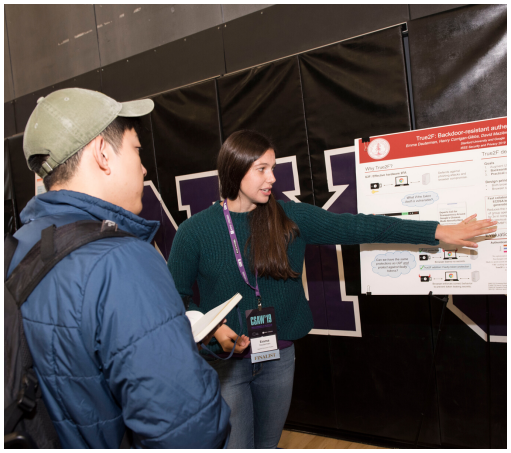
As an added highlight, Red Balloon Security ran its own contest, challenging participants to figure out a way to breach a real ATM machine stocked with $2 bills. A total $2,000 was dispensed to those who correctly cracked the machine's password.

Five other sites around the world, including Europe (Grenoble-INP Esisar in France), India (IIT Kanpur), the Middle East and North Africa (NYU Abu Dhabi), Israel (Ben-Gurion University and other locations) and Mexico (Universidad Iberoamericana) held their own versions of CSAW during the same calendar period. Each hosted from two to four competitions, along with other educational, professional, and social activities.

This newsletter highlights a handful of stories from CSAW 2019. For a complete list of winners, as well as photos from all the host sites, go to the CSAW web site at https://csaw.engineering.nyu.edu/. Note that **CSAW 2020 will return to the same six location from November 5 to 7, 2020.**

POLICY AND APPLIED RESEARCH COMPETITIONS TOPICS REFLECT "OF-THE-MOMENT" CONCERNS

The papers that captured top honors in CSAW's 2019 Applied Research and Policy Competitions deal with a broad range of research issues, but one common thread is the timeliness of their topics. Collectively, the presentations offer an up-to-minute perspective of the threats that keep cybersecurity professionals awake at night.



1st Place recipient Emma Dautemann (CSAW-US/Canada) shares her research on backdoor-resitant authentication tokens

The first place presentation in the U.S.—Canada competition dealt with the possible risk of relying on hardware components as part of a two-factor authentication system. As stated by its lead author, Emma Dauterman of Stanford University and Google, who presented the paper, "This raises the question: Can we enjoy the benefits of hardware-level security protections without incurring the risks of introducing additional (and often untrustworthy) hardware components into our systems?" Her paper aimed to provide "a strong positive answer to this question for the interesting special case of hardware authentication tokens" by presenting True2F, a token designed to resist backdoor tampering. Other finalists addressed attacks on Voice Processing Systems via injection of hidden commands, and vulnerabilities in virtual personal assistants, such as Amazon Alexa and Google Assistant.

Meanwhile, the winning presentations at other global competition sites also pursued timely themes. At CSAW Europe, the winning presentation by Vladislav Mladenov et al from Ruhr University Bochum, focused on methods by which PDF signatures could be spoofed, while at CSAW India, Sharad Joshi of IIT Ghandhinagar took first place honors for a presentation that utilized a neural network-based approach to verifying the authenticity of printed text documents that have been captured by smartphone cameras and shared over a messaging platform. At CSAW MENA (Middle East and North Africa), a team of students and faculty from Khalifa University and NYU Abu Dhabi, led by Lilas Alrahis, took first place for a paper that demonstrated how scan obfuscation techniques used on computer chips can be broken. Lastly, at the CSAW Israel competition. Amit Klein and Benny Pinkas presented a new tracking mechanism that can cross private browsing boundaries across different browsers and multiple networks.

Themes in the policy competition were equally au courant. The finalists addressed such topics as detecting deepfakes in political advertising; assessing and limiting privacy concerns connected to the NSA Prism surveillance program; the need for more stringent regulation governing the storage, transport, and usage of genetic information, particularly such information acquired by companies doing genetic testing; the need for appropriate cyber responses for illegal acts that fall below the level of armed conflict, and improving data security in small businesses.
Most of the winning papers from the CSAW sites can be accessed at https://csaw.engineering.nyu.edu/.

From NYU Abu Dhabi, 1st place winners Hack 3D Pedro Velasquez and Cole Beasley

Growing New Competitions to Meet New Threats: A Look at the Genesis of Hack3D

The goal of CSAW, the world's most comprehensive student cybersecurity games, held each fall at the NYU Tandon School of Engineering, has always been to educate, but as the event has evolved, it's not just students who are learning the lessons. Over the past few years, CSAW has launched new competitions to educate cyber professionals about emerging risks to digitally locked computer chips and machine learning programs. But, Hack 3D, which debuted as a pilot competition last year, has targeted a vulnerability that spans engineering disciplines. And its creator and faculty lead, Nikhil Gupta, hopes the competition will serve as a wake-up call to a manufacturing sector that has perhaps been lax in acknowledging cybersecurity threats.

Gupta, also a professor in NYU Tandon's Department of Mechanical and Aerospace Engineering, has published a number of papers about new security methods for 3D printing, and his work has garnered several grants in collaboration with Dr. Ramesh Karri, also an NYU Tandon professor of Electrical and Computer Engineering. Yet, he became aware that "manufacturers did not see the threat," despite rampant theft of intellectual property, even at the nation state level, which he characterized as "foreign jets that looked a lot like ones manufactured in the U.S." This year's Hack 3D Challenge directly addressed issues of intellectual property theft, as the final round asked competitors to hack an anti-counterfeiting strategy. By having students attack such strategies, Gupta hopes to create awareness of the very real threats to manufacturing and to "create ambassadors for security."

Recruiting ambassadors, however, meant creating and maintaining excitement about the work. For Gupta, this meant ensuring participants didn't lose their "level of excitement and engagement" as they walked through the steps of the competition. To avoid this problem, he notes, "We borrowed an approach from video games, in which every time the students completed a task, they were rewarded with a key to unlock the next level."

Engagement did not appear to be a problem for this year's Hack 3D winners, Cole Beasley and Pedro Velazquez. (Second and third place went to the pwndevils of Arizona State University and team AGGIES of Texas A&M University, respectively.) As quoted in a press release from his home school, NYU Abu Dhabi, Beasley points to the need to "think and approach the presented problem with differing skill sets to complete one single task," as one element that made his time at CSAW such a great experience. Indeed, the cross-disciplinary nature of the challenge offers its own benefits. "When these students enter industry, they'll need to work with engineers and scientists from many different disciplines," Gupta observes. The Hack 3D participants "have already had the advantage of working with engineers with varied types of expertise."

Gupta comments that he was happy overall with the response to this year's competition, pointing out that 19 teams participated, and the total might have been higher had it not been for an initial problem with the link for registration. "We also disseminated the files to anyone who wanted them, whether they were part of the contest or not," he adds, noting that doing so enabled the planning team to solicit a lot more feedback.

Additive manufacturing is credited by one study to have been a $9 billion industry in 2019, so the time is certainly right to seek security ambassadors. Hopefully, this year's participants are ready to spread the word.

USNA CONTINUES TO SAIL THROUGH POLICY COMPETITION

The 2nd place winners from USNA presenting at the Policy Competition: (l to r) Midshipmen Rae-Kelly Hamilton, Ian Flynn, Byron Gallagher, Anthony Perry

The motto of the United States Naval Academy is "Ex Scientia Tridens," which translates from the Latin to "From Knowledge, Seapower." The military academies of the United States have long been celebrated for producing talented engineers to create and direct power of all sorts, be it through energy, communications, or weaponry. But now, a new generation of midshipmen are powering our nation's defense with a different type of knowledge: an awareness of the legal, ethical, and policy factors that can influence and underscore how and when such defenses are deployed. And, armed with this new approach, the venerable Annapolis, MD, school has become a perennial winner in the CSAW Policy Competition. Since they first participated in 2014, the midshipmen have never failed to place in the Policy Competition. They collected 2nd and 3rd place in their inaugural event, 1st place in 2015 and 2017, and 2nd and 3rd place in 2016, 2018 and 2019.

When asked about this impressive track record, Jeff Kosseff, an assistant professor of Cybersecurity Law at USNA, who serves as faculty advisor to the teams, points to the interdisciplinary nature of the academic major in which the teams' members are enrolled. "The students who compete in the CSAW policy competition major in cyber operations, an ABET-accredited major at the Naval Academy," he explains, noting that about one-third of the curriculum for this major consists of courses in social engineering, cyber law and ethics, and cyber policy. Midshipman Anthony Perry, who along with his colleagues Ian Flynn, Byron Gallagher, and Rae-Kelly Hamilton took second place in the 2019 competition, concurs that "a diverse knowledge of the cyber domain," such as what this course provides, "leads to greater success."

While their course preparation at the academy may be an advantage, all the participants acknowledged garnering awards in the competition is not a cake walk. According to Kosseff, the midshipmen pick their own topics for the competition, based on their own interests. And, this takes time. Midshipman Perry admits, "It was difficult to hone our project, as there is so much in cyberspace that has yet to be discussed. We spent several hours simply directing our ideas into a cohesive idea." Making sure the topic is relevant and important adds a level of difficulty to the process as well. Midshipman Flynn observes, "We were looking for something that was applicable and an actual need within government today, " and the topic they finally ended up pursuing, "was one of the recurring issues we had heard during class and in lectures—that many countries do not have set structures to respond to and prevent cyber attacks." The resulting presentation, Flynn notes, "established international norms to create a response model to cyber-attacks."

The USNA team that took third place—Midshipmen Kameron Chumley, Cameron Cook, Brendan Reilly, and Brendan Henry—picked an equally timely topic. Their presentation focused on a recommendation to use hashing to ensure the validity of political advertising so elections are not unfairly manipulated.

Picking the right topic and committing significant amounts of time is not the only hurdle Policy teams need to overcome. Kosseff notes, "This is often the first policy competition in which the midshipmen have participated, so for some it is a bit anxiety-producing to present about cutting-edge cyber topics to an audience of truly expert judges." In addition, Kosseff points out that participants need to learn how to consider the awareness of their audience, including that of the judges. "They may have immersed themselves in the subject for weeks, but their audience may be new to their presentation topic." The students have to be sure their "written and oral presentations are accessible to all audiences, focusing on clarity and conciseness."

With everything else these future Naval officers have to consider, it would be reasonable to ask whether the effort involved is worth it. Dr. Andrew Phillips, academic dean and provost at USNA, says yes. "Naval Academy graduates are destined to serve their country as leaders of sailors and marines," and so the academy places "a premium on their ability to develop and articulate sound, principled strategies to solve problems." He adds, "The CSAW competition is one of the best ways we have to test the success of our educational approach against everyone else's. So, we are gratified to be part of the competition, and even more so that we do well every year." Kosseff cites the competition as providing the midshipmen "with an excellent opportunity to develop their analytical skills" by "stressing the importance of effectively communicating their ideas in writing and oral presentations."

Perhaps Midshipman Rae-Kelly Hamilton provides the best answer as to why the CSAW Policy Competition matters. She states that it "provides an engaging mission for midshipmen to approach in a collaborative manner, forcing them to holistically consider the problem set, and present both findings and recommendations in a way mirroring the requirements for communication and innovation demanded by our future jobs in the Fleet. "

CSAW CONFIDENTIAL: WINNING AT CTF IS ALL ABOUT THE PRACTICE

The Perfect Blue Team

Want to win at Capture the Flag (CTF)? Team Perfect Blue, who took first place honors in not only CTF, but also in the Security Quiz, has a rather simple answer: Just keep playing. The team, whose members all attend different colleges, credit frequent participation in other CTF competitions for their success. The squad estimates that they have completed about 50 CTF competitions since they became a team or, as Sampriti Panda of Drexel put it, "most every weekend, we're playing." As a result, the group went from "No Names in 2018," to #9 on the CTF World Leader Board. Stephen Tong of the Georgia Institute of Technology adds that building "interpersonal skills" is also a key. "Fundamentally," he observes, "it is a social activity. It encourages you to keep studying to share with others, within a circle of people who help you to filter information." In short, Tong suggests, "80% of success is just talking to people."

Perfect Blue—whose other members are Alex Lin (Purdue University), Kevin Shen (University of Maryland), and Jasraj Bedi (University of Waterloo)—got its name from a 1997 Japanese film, and came together during the High School Forensics (now Red) competition at the 2017 edition of CSAW. As both Sampriti and Stephen pointed out, "Each of us was the only person from our high school that did CTF competitions." One year later, they returned to CSAW and placed third in the CTF.

In late January of this year, Perfect Blue met up for a conversation with CyberByte to provide some insights on their success. Here are a few of their comments.

Q: How do you divide up the work?
Alex: There are four categories—web exploitation, binary exploitation, reverse engineering, and cryptography. Each of us takes one category. Usually we will each work in our own category for the first 24 hours, then we pitch in to help where needed.

Q. Do you take turns grabbing naps over the 36 hours?
Jasraj: We all stay awake as long as we can, at least for the first 24 hours.
Sampriti: At the last competition, Alex and I worked for six hours and then slept for a few hours, maybe four.

Q. Does the competition have to be done in any fixed order?
Kevin: It is done Jeopardy style, so you can pick the categories and point values. There's no real order.
Sampriti: Each challenge is independent, All that matters is whether you solve it or not.

Q. How did you prep for the CTF finals? Was there anything special you reviewed or looked over?
Jasraj: There is really no way to prep because there is no way to know what the questions will be.
Sampriti: You can look at challenges from other CTFs.
Kevin: For the trivia competition, we did do some preparation. When we knew IBM was hosting, we looked at events in cybersecurity from that company.

Q. Any other keys to success?
Kevin: A lot of it comes with experience. After a while, you begin to recognize layouts of code. Skill is mostly familiarity.
As all the members of Perfect Blue are underclassmen (four sophomores and one freshman), all said they plan to be back for CSAW 2020.

Some Additional Thoughts from CTF Co-Lead, Leon Chou

To amplify Perfect Blue's comments, we checked in with Leon Chou, who along with Kent Ma served as co-lead on the CTF competition. Here are a few of his thoughts on creating the challenge, takeaways from the competition, and some advice on how to win.

"CSAW CTF tests the knowledge and skills of its competitors, and gives them the opportunity to exercise niche skills, such as low-level exploitation, which is rare in real-world security. These CTFs are designed to be a safe place to present those tests.

In developing the scenarios, we separate challenges by category, and develop our challenge board, using a loose set of point value slots. Specific categories have specific criteria, but we attempt to stick to a fairly consistent lineup. One of the most important factors of challenge development for us is to make sure the challenge is obvious to solve, but the methodology is difficult. The CTF is not intended to be a guessing/trivia game.

However, in developing challenges, it is simplest to start from a specific vulnerability or bug class, and then iterate on the steps to get there. Being able to isolate a bug and then present it to the competitors asking 'can you exploit this?' is something that demonstrates their ability to understand and adapt exploits.

We want participants to leave motivated to come back better next time, and we want the winners to feel like they earned their victory, and that they need to work just as hard to keep their spot. The key to excelling is to practice and learn as much as possible. The CTF scene is one that can be learned, but there are no shortcuts to learning each of these topics."

Both Sides Now: Former Embedded Security Champ Designs 2019 Competition

By Nektarios Tsoutsos, Global Lead, 2019 Embedded Security Challenge

In 2013, then NYU Ph.D. student Nektarios Tsoutsos entered the CSAW Embedded Security Challenge. He not only took the first place title that year, but also began an affiliation with CSAW, and with this particular competition, that six years later took him from solving the challenge to creating it. Now an assistant professor in the Department of Electrical and Computer Engineering at the University of Delaware, with a joint appointment in the Department of Computer and Information Sciences, Tsoutsos served as the Global Lead on the 2019 Embedded Security Challenge. As such, he was responsible for overseeing the competition at three sites: Brooklyn, France, and India. CyberByte invited Tsoutsos to share his thoughts on why CSAW remains important to him, and how this year's challenge came about.

"I immediately understood that CSAW was much more than a student competition: it was a forum to talk about cybersecurity, a unique opportunity to meet peers and area experts, and a driver for state-of-the-art research. For example, the 2013 topic was about circumventing a recently published security protection mechanism that defends computer hardware. From that point on, I knew that CSAW was one of the most important security events in the region. Following the 2013 win, I was invited to be the ESC challenge leader. From that position I was able to develop unique challenges on important areas of hardware-oriented cybersecurity, and helped organize the event in 2015, 2016 and 2017. When I joined the faculty at the University of Delaware in 2018, I was able to join CSAW again in a different role. This time, I advised three talented cybersecurity students from UD. That year the competition focused on exfiltrating information from secure areas using IoT light bulbs, and the UD team received first place honors. Then, in 2019, I was excited to join the CSAW organizers and become the faculty guide for ESC. I have been working with the amazing CSAW team at Tandon for many years and taking over the organization of the competition was a great opportunity to give back to this community and continue to engage with students and cybersecurity professionals.

The development of an ESC challenge takes into account many criteria. First, the cost of materials and computing resources should be reasonable. In some cases, the materials available in the US can not be accessed in all other regions and we have to consider the trade-off of shipping from the US or choosing different hardware that is readily available in other parts of the world. Likewise, we have to consider the entry cost for students: if a student needs to pay an upfront cost to have access to special software or hardware, this would affect our goal of reaching as many students as possible every year.

This year we reached more than 100 students across 28 teams on three continents. The 2019 finalists developed state of the art solutions to reverse engineer a custom computer board, and these results are very useful for the cybersecurity community.

With respect to time, the organizing team starts very early each year and we always expect organization to be a multi-month process. Given our experience so far, we can now tweak each year's challenge development to fit these timelines. The two student leaders from the ECE department at the University of Delaware developed a custom computer board under my supervision, an effort that took several months. For each iteration we had to wait for the factory to fabricate the boards and then ship them to UD for testing. Having a custom computer board to hack makes the competition unique and gives its creators the freedom to define more interesting challenges.

Each year, the faculty guide of ESC researches different challenge ideas and identifies the one that is the most promising. A lot goes into this decision, including current events and security trends. Like many professionals in the field, I have been excited about RFID security for many years, given its ubiquitous use in such applications as access control in buildings. Moreover, an RFID challenge also offered a lot of freedom on how the participants could solve it, and this is why this topic was ultimately selected for ESC 2019.

I would say the primary takeaway from the competition, as a student, was building a security mindset, which is one of the goals of the event. CSAW's objective in training the cybersecurity professionals of tomorrow and building the proper mindset (essentially the ability to think like an attacker and predict their next move) is a big part of this process.

Comments or Questions? ccs@nyu.edu

Visit cyber.nyu.edu for more information on
how to apply for our programs and scholarships

CSAW 19'

BROOKLYN

CSAW 19'

INDIA

CSAW 19'

MEXICO AND EUROPE

Center For Cybersecurity
Industry Partners & Sponsors