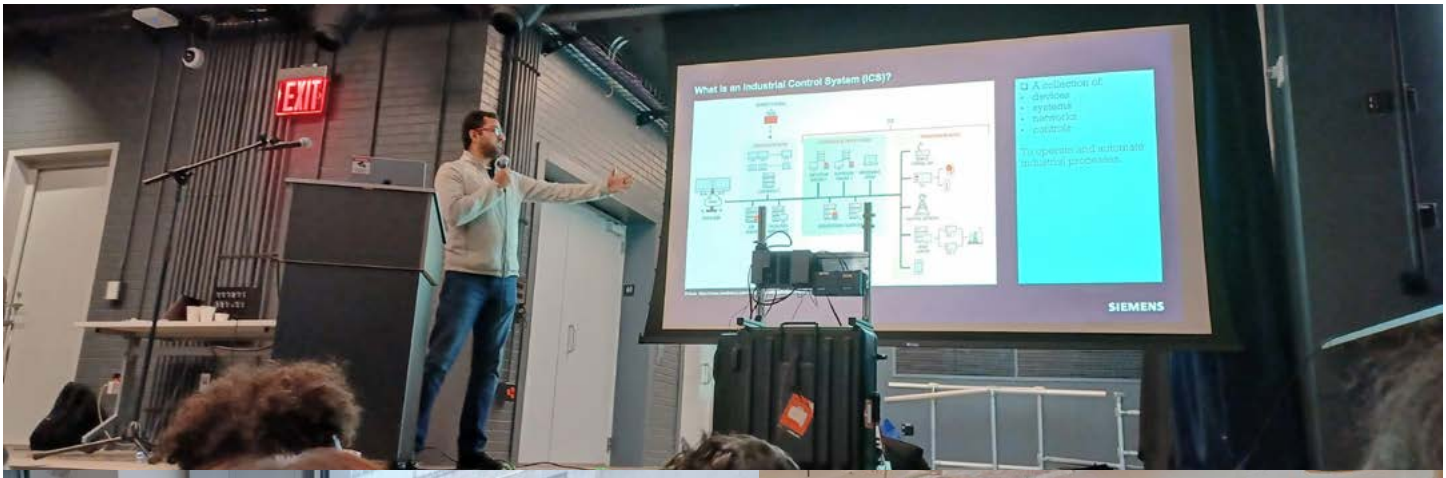
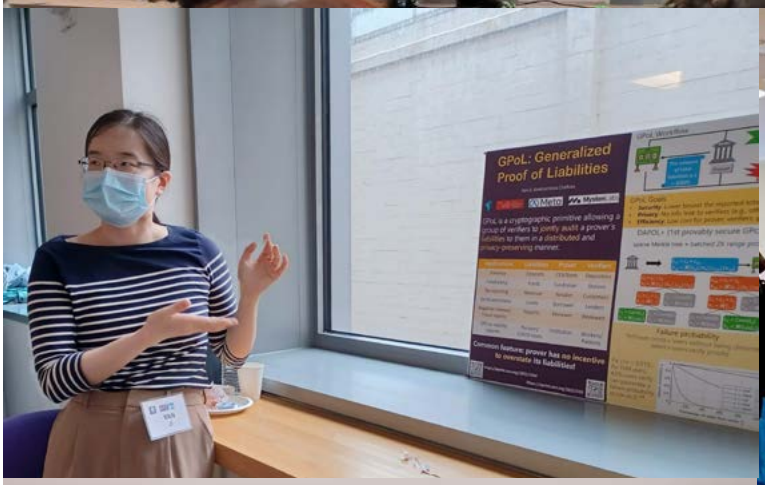
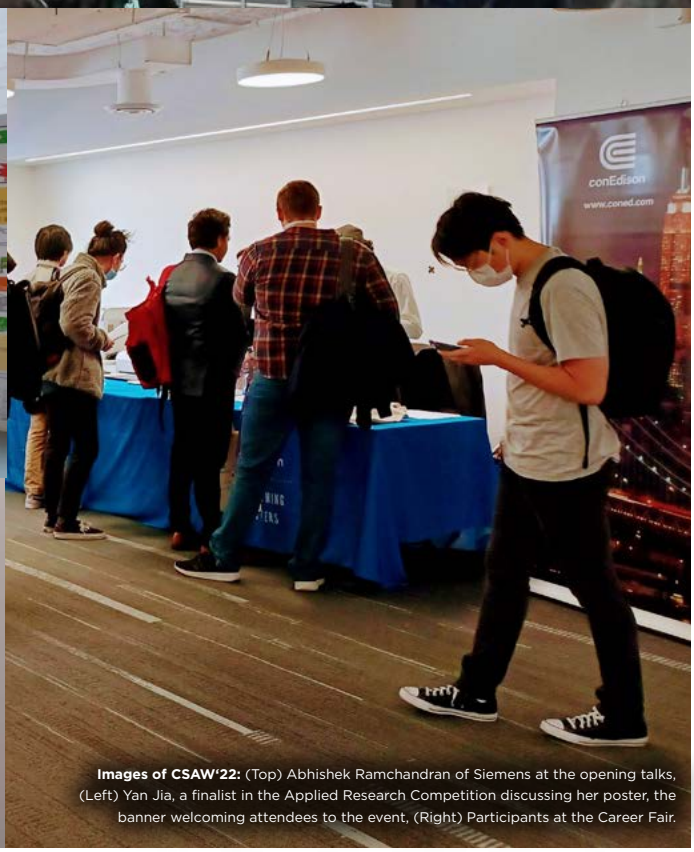
CYBERBYTE







Images of CSAW'22: (Top) Abhishek Ramchandran of Siemens at the opening talks, (Left) Yan Jia, a finalist in the Applied Research Competition discussing her poster, the banner welcoming attendees to the event, (Right) Participants at the Career Fair.

WELCOME BACK, CSAW

CENTER FOR
CYBERSECURITY

NYU | TANDON

"ALEXA: WHO ARE YOU TALKING TO?"

As smart devices grow more ubiquitous in our homes, workplaces, and even our forms of transportation, the potential for all sorts of mischief—from leaks of personal data to the ability to remotely step on the brakes of a fleet of cars—grows with it. There is no doubt that these connected devices do make life easier, but is convenience an adequate tradeoff for the increased security and privacy risks they might bring with them? This tradeoff becomes harder to assess in cases where the end user might have little or no control over the connected device in question, such as with infusion pumps or ventilators commonly used in hospitals, or the electronic control units in vehicles.

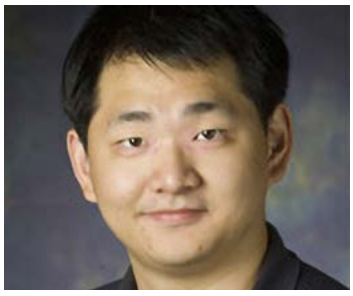
Thanks to the work of several researchers at the Center for Cybersecurity, we now know a lot more about the behavior of smart devices and are finding ways to prevent their intrusion into our data, our safety, and our security. In this issue, you'll learn more about *IoT Inspector*, the data collection tool invented by Tandon assistant professor Dr. Danny Y. Huang to open up the "black boxes" that are our smart devices and find out who they are talking to. You'll also learn how Dr. Justin Cappos, newly christened a Tandon "Agent of Optimism" (see a related article later in this issue), is defending other devices on the Internet of Things through the Uptane project. Lastly, we check in on the work of one of my Ph.D. students, Yuhan Zhao, who has designed and tested a game framework that enables a holistic risk assessment of ransomware in networks and a cross-layer design of cyber defense and investment strategies to mitigate the attack.

This issue also features highlights from the 2022 edition of CSAW, the first conducted in-person in two years, as well as profiles of Ph.D. candidate Animesh Basak Chowdhury and CCS alumnus Dr. Kevin Gallager. Enjoy!

Dr. Quanyan Zhu, Editor in Chief

IN THIS ISSUE

STAFF



Editor in Chief

Quanyan Zhu

Editorial Copy Writer

Lois Anne DeLong

RESEARCH FOCUS:

HOW CCS RESEARCHERS ARE HELPING US STAY SMARTER THAN OUR SMART DEVICES

Defending against the threats engendered by connected devices becomes easier and more successful if one can fight on several fronts. Through the efforts highlighted below, as well as the initiatives led by Dr. Danny Y. Huang (see the accompanying profile on page 6), CCS researchers are offering a clearer picture of how IoT devices function, and how any threats they engender can be countered

Figure showing the principal components of the Uptane secure software update systems.

SECURING SOTA UPDATES

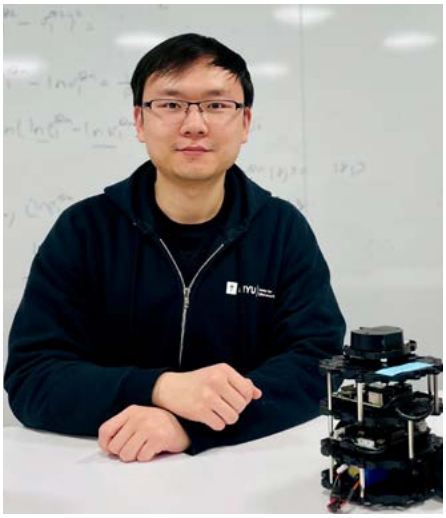
With perhaps as many as 150 distinct Electronic Control Units (ECUs) (see https://www.eenewseurope.com/en/number-of-automotive-ecus-continues-to-rise/) that are either directly connected to the Internet or receive updates via software over the air (SOTA), an automobile can be thought of as a network of IoTs on wheels. Unfortunately, a remote hack on these ECUs, particularly one engineered by sophisticated nation-state actors, can lead to injuries or loss of life. For example, imagine a fleet of police cars all being locked at once, trapping the officers inside...or perhaps locking them out.

Uptane, an open source software update framework, has been countering these types of threats to automobiles for seven years. (https://uptane.github.io/) Developed by Dr. Justin Cappos, associate professor of computer and systems engineering at NYU Tandon, Uptane protects ECUs by creating a series of hurdles that potential attackers must leap before they can cause any real damage. The framework, based on an earlier Cappos project called The Update Framework (TUF), builds compromise resilience into software update systems, making it not only wharder to take down, but also easier to recover afterward. (https://theupdateframework.io/) The framework was originally developed under a grant from the U.S. Department of Homeland Security, and in collaboration with researchers from the University of Michigan Transportation Research Institute and the Southwest Research Institute. Since then it has since been integrated into Automotive Grade Linux (https://www.automotivelinux.org/), an open source system currently used by many large automotive manufacturers. In addition, multiple different open source and closed source implementations have also been developed for the automotive market.

Now, potential IoT applications outside of the automotive world are emerging. Torizon, a new Linux product development platform (https://www.toradex.com/torizon) from a multinational embedded hardware and software manufacturer called Toradex (https://www.toradex.com/about-toradex), is bringing Uptane technology to markets such as industrial automation, medical and health care equipment, and smart city devices, such as street lights, electric charging stations, and camera systems. Torizon adapts one of Uptane's earliest commercial integrations, Aktualizr, which was initially developed by Advanced Telematics Systems (later HERE Technologies https://developer.toradex.com/torizon/torizon-platform/torizonupdates/aktualizr-modifying-the-settingsof-torizon-ota-client/).

As Uptane is an open source technology, it isn't possible to track all the applications currently using it to protect IoT applications. But, recently the research team has learned about emerging implementations in robotics, and aerospace. "It's remarkable to me how much impact you can have by building a broad community around an open and free security system like Uptane," said Professor Cappos. "It seems like everytime I go to a conference, someone approaches me and talks about a new use case for the technology."

Dr. Justin Cappos



Ph.D. Candidate Yuhan Zhao,

ENSURING CRIME DOESN'T PAY

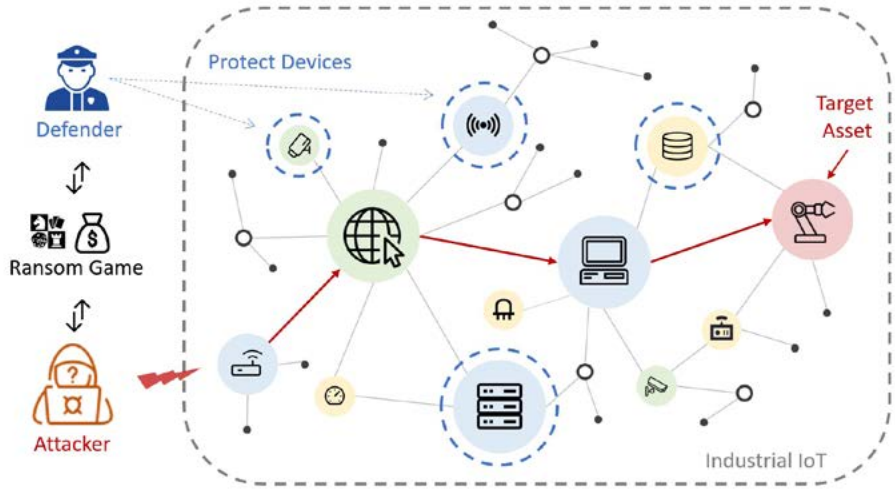
In Dr. Quanyan Zhu's LARX laboratory, the development or enhancement of secure, resilient, and sustainable dynamic systems and networks often involves the application of game theory. In one of the most recent examples, Yuhan Zhao, a Ph.D. candidate advised by Huang and affiliated with LARX, has harnessed this theory for a strategy that can neutralize the threat of ransomware. Essentially, Zhao's work offers a way to remove the profit potential from these attacks, and thus discourage their execution.

Zhao's work, coauthored by Zhu and Ph.D. student Yunfei Ge, was presented at the International Conference on Decision and Game Theory for Security in 2021 (https://par.nsf.gov/servlets/purl/10312134). We asked Zhao to explain the strategy in his own words:

"We initiated this study in the wake of a series of ransomware attacks in IoT applications, including the one on Colonial Pipeline that caused gas shortages and price increases. Unlike many works focusing on the technical approaches to prevent ransomware attacks, we set out to study high-level behavioral strategies to prevent and mitigate ransomware attacks on IoT from an economic perspective. We analyze the operator and the attacker's behavior, and then abstract the spreading process as a series of interactions between the two parties. These interactions can be modeled as a dynamic game between the amount the operator invests in security and the probability of being affected. If there is no sufficient security investment, ransomware has a strong probability of compromising the target assets. In this case, the interaction between the operator and the attacker concerns whether or not the attacker will profit from the attack. We use another game model to find the best ransom payment strategy for the operator to minimize the loss. We also estimate the worst ransom that could be demanded by the attacker.

We tested our nested game model with a simple but typical IoT network. In doing so, we determined the operator's best security investment strategy to prevent ransomware from spreading, as well as a ransom payment strategy to mitigate attack loss with both a limited and unlimited budget. Lastly we used the prospect theory to analyze how human cognitive factors can affect security investment and ransom payment strategies. Using simulations, we evaluated the performance of the cyber MG defense mechanism, which serves as the cyber risk assessment for future security decision-making."

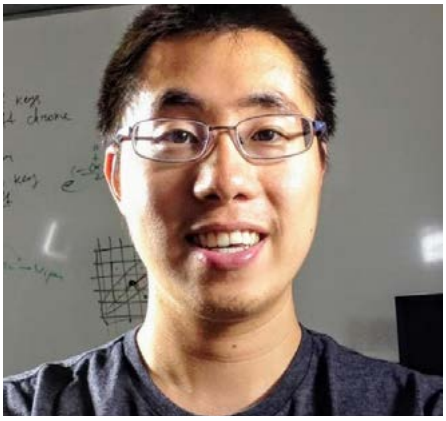
In addition to Zhao's work, the LARX lab has also contributed a chapter to the text *IoT Supply Chain Security Risk Analysis and Mitigation*. Written by Dr. Zhu, along with two CCS alumni, Timothy Kieras and Dr. Junaid Farooq, it tackles what the authors describe as "the next frontier of threats in the rapidly evolving IoT ecosystem."



Schematic of a ransomware attack, showing the goals and actions of the hacker and the defender.

FACULTY PROFILE:

DANNY Y. HUANG



SETTING GUARDRAILS ON THE INTERNET OF THINGS

As documented in the Fall 2022 issue of *CyberByte*, protecting privacy requires a diversity of approaches. Dr. Danny Y. Huang has mapped out a somewhat unique territory within this field: identifying the types and amounts of data being obtained and shared through smart devices connected to the Internet of Things (IoT). As he titled one talk about his work, his research is all about "watching the IoTs that watch us" and sharing whatever is learned with everyday consumers. With students and colleagues in his mLab (https://mlab.engineering.nyu.edu/), he is committed to using empirical measurements derived from real-world implementations to evaluate and address privacy threats.

According to Huang, his journey to this particular privacy niche was a natural evolution from the investigations of internet abuses and cybercrimes he had conducted as a Ph.D. candidate at the University of California-San Diego. When he moved on to a post-doctoral position at Princeton University in 2017, it was at a time when hacks of nanny cams were dominating news reports. Huang recognized these attacks as a "more insidious way for consumers to be affected" than previous thefts of personal data. The difference was the involvement of third-parties. "These devices are just black boxes that sit in a corner of someone's living room and that individual has no way to find out what's going on," he explained, in response to a series of questions *CyberByte* asked about his work. Though he acknowledges that tools, such as Wireshark or TCPDUMP, which can look into these devices already exist, "these are professional tools which even a researcher like myself find difficult to use. There is no way to just quickly inspect what this device is doing so the consumer knows if he/she should return it." Thus, his new research direction had a dual purpose: to establish "a way for consumers to find out what's going on behind the scenes of these devices with just a few clicks," while also compiling "a large amount of real data from real IoT devices."

To achieve both these goals, Huang built a tool called *IoT Inspector* (https://inspector.engineering.nyu.edu/), an open source desktop application that "helps consumers understand what's going on in their house by just visualizing the traffic." He explains the device with the following example: "Suppose you have 10 different smart devices in the house. Using *IoT inspector*, you can see 'Oh, I have this camera that is sending my traffic unencrypted to a particular country. I don't trust that country, so I should get rid of this device'." Furthermore, the software also "allows consumers to donate the data they collected to researchers." For researchers, its data collection value is equivalent to "moving my research lab into about 7,000 homes every day, sharing data from about 65,000 different devices." Financed in part by the Alfred P. Sloan Foundation through the Consumer Reports Digital Lab Fellows program, Huang and a number of other faculty at seven universities have utilized *IoT Inspector* to build "one of the largest open datasets of IoT traffic in the entire world."

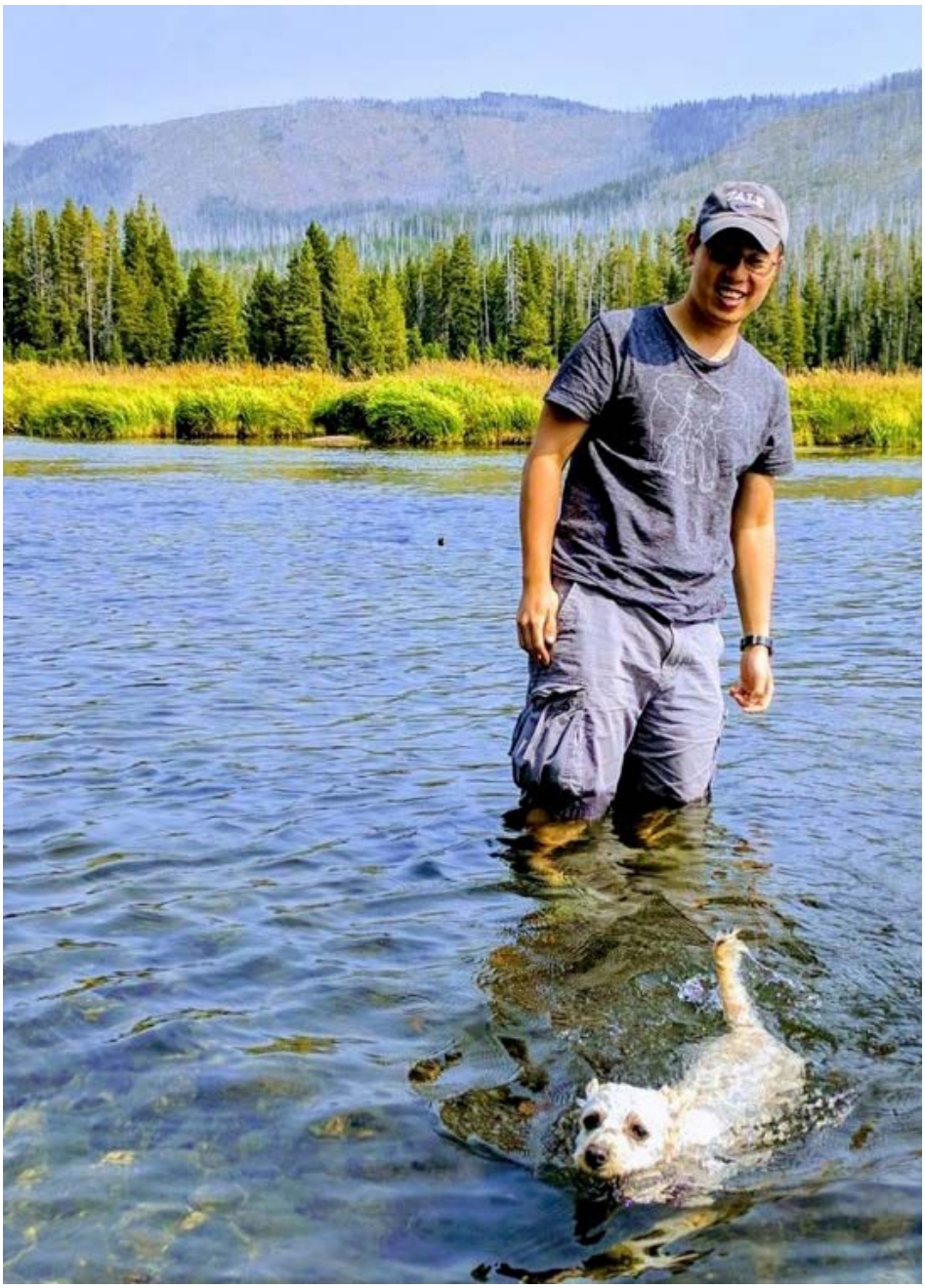
An initial analysis of that dataset (https://mlab.engineering.nyu.edu/static/ubicomp-20.pdf) found that "many device vendors, including Amazon and Google, use outdated TLS versions and send unencrypted traffic, sometimes to advertising and tracking services." The researchers saw similar traffic patterns in smart TVs from at least 10 vendors. Lastly, the paper reported "widespread cross-border communications, sometimes unencrypted, between devices and Internet services that are located in countries with potentially poor privacy practices."

More recently, Huang has been focusing on more subtle intrusions by IoT devices into the life of individuals and families. As a new parent with a young daughter, he became a bit troubled about certain "skills," or third-party functionalities on voice personal assistants (VPAs) like Alexa. "I was reviewing data from real users that suggested Amazon doesn't

really have a good vetting process for these often third-party skills." So, he built a natural language processing-based system called SkillBot and had it interact with VPA apps. In analyzing the conversations between these machines, his research team found, "28 risky child-directed apps" and compiled "a growing dataset of 31,966 non-overlapping app behaviors collected from 3,434 Alexa apps." While acknowledging that gathering this type of data can not necessarily force a company to do a better job on vetting these skills, it is "a way to generate buzz, publicity, and transparency into an otherwise quite opaque ecosystem." (You can read more about Skillbot in an *ACM Transactions on Internet Technology* article that is available as a PDF at https://arxiv.org/pdf/2102.03382.pdf.)

The value of "generating buzz" is that it can sometimes lead to actions despite corporate opposition or apathy. Huang notes that because of his work with *IoT inspector* and Smart TVs, the Federal Trade Commission asked him to give a talk that could help the agency determine if these devices might be in violation of the Children's Online Privacy Protection Act (https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa). It's one example of the many "intersections" at which his research efforts sit. Another is his somewhat unusual appointment to both the Electrical and Computer Engineering and Computer Science and Engineering departments at Tandon. When asked about this arrangement, he attributes it to his research initiatives embodying not only an understanding of IoT tools, but also of the people who could be threatened by these tools. "I believe that's where the computer science aspect of my work comes into play, where we try to understand human behaviors, be it children, or Airbnb guests," he explains, the latter category referencing another emerging privacy concern—hidden cameras in Airbnb apartments.

Currently, he is applying that human understanding to a unique form of "high-tech domestic abuse" as he called



Huang enjoys some time off with 'Dr Momo,' the namesake and Supreme Director of mLab.

it in which former intimate partners are using IOT devices like smart thermostats or air conditioners to harass their exes. This research is documented in a paper to be presented in August at the USENIX Security Conference in Anaheim, CA.

So, with all the potential risks to privacy, security, and personal comfort, should we even be using Alexa or any of her smart device sisters? Huang suggests it's a matter of each individual's comfort level with "reasonable risks." "Not all IoT devices have built in risks, or risks large enough for alarm. I use a ton of smart plugs to turn lights on and off. Sure, they're privacy risks because these companies may know what time you turn off lights, but I am okay with that reasonable risk. I just think we need to be a little bit careful as to what kind of devices are involved, especially if they're cameras."

PH.D. PROFILE:

ANIMESH BASAK CHOWDHURY

A WINNING COMPETITOR FOCUSED ON CREATING STRONGER, SMARTER CHIPS

Animesh Basak Chowdhury is a Ph.D. candidate in Electrical and Computer Engineering at the NYU Tandon School of Engineering, where he works with Drs. Ramesh Karri and Siddharth Garg on projects involving machine learning for chip design, and secure Electronics Design Automation (EDA). Prior to joining the Ph.D. program at Tandon in 2019, he completed an MS in Computer Science at the Indian Statistical Institute in Kolkata, and worked for three years as a researcher at the Tata Research Development and Design Centre (TRDDC) in Pune, India. Over the past few years, Animesh has excelled in a number of software verification and testing competitions, most recently as part of a team that came in third at the helloCTF 2022 competition. *CyberByte* touched base with Animesh earlier this year as he enters what will likely be his final semester at Tandon to talk about his research interests, why he chose to pursue a Ph.D. here, and where his plans might take him after leaving Tandon.

CyberByte: Let's start with your core research interests. Can you define them for me?

Chowdhury: I work primarily in the area of Electronic Design Automation (EDA). EDA automates the production of high-quality electronic chips in a shorter time frame with fewer errors. It employs software tools to manage complex tasks, such as design, synthesis, verification, validation, and testing. EDA tools generate the physical layout of the system, which is verified to meet design specifications of industry standards. Finally, the EDA tools are used to test and validate the system's functionality before it goes into production, saving time and money, and ensuring that the final product meets customer requirements.

My area of research involves utilizing machine learning in two crucial stages of EDA: logic synthesis and testing. These challenges have a complexity level that makes them difficult to solve. To overcome this, leading companies, such as Synopsys, Cadence, and Mentor Graphics, rely on well-established heuristic algorithms to produce high-quality, yet sub-optimal solutions.

Recently, the rise of machine learning has sparked renewed interest in these combinatorial optimization problems, and my research focuses on using past data to enhance the search algorithm's exploration strategy. This reduces the runtime while maintaining similar quality. Additionally, I analyze the quality of solutions generated by deep learning techniques, and assess their robustness.

Robustness in ML algorithms are crucial as low quality solutions would incur heavy costs in terms of power/performance/area and coverage statistics.

CyberByte: What was the primary motivation for pursuing a Ph.D.? And what drew you to Tandon in particular?

Chowdhury: Following the completion of my Master's degree in Computer Science in 2016, I worked as an industrial researcher at the Tata Research Development and Design Centre (TRDDC) in Pune, India for three years. I wanted to gain some research experience before fully committing to a PhD program, and learn how to conduct research systematically. I also wanted to improve my communication and dissemination skills.

My decision to apply to Tandon has a unique backstory. In 2018, while I was submitting applications, I was particularly interested in the application of machine learning in EDA due to my prior experience in VLSI testing and verification and validation. These earlier projects showed me the potential for machine learning in this interdisciplinary field. Tandon's Department of Electrical and Computer Engineering has a faculty member, Siddharth Garg, who is knowledgeable in both machine learning and EDA (having completed his PhD thesis in EDA). This made him an ideal advisor for me, so I decided to apply under his supervision.

CyberByte: It seems you excel at professional competitions, such as Hack @ DAC. How did you become involved in these competitions? Do you think they have enhanced your understanding of real-world security issues?

Chowdhury: I was introduced to international competitions while working at TRDDC, particularly SV-COMP (International Competition on Software Verification) and TESTCOMP (International Competition on Software Testing). These contests challenge participants to find bugs in software. Many software verification and testing groups from around the world participate in these contests, and their tools are evaluated on over 10,000 pieces of code. In 2018 and 2019, I participated as part of a group in these contests and we came in first both years. In 2019, I also participated solo in the Rigorous Examination of Reactive Systems Competition, and came in second place overall. After starting at NYU, I took part in Hack@DAC in 2020 and 2021, an event billed as the world's largest hardware security Capture the Flag competition, and bagged second and third place, respectively. Last month, our team also won third position in the helloCTF 2022 competition, bagging a $5,000 cash prize (https://helloctf.org/22/). (You can watch Chowdhury discuss his winning strategy in the HACK@ DAC competition In a podcast segment of Intel's Cyber Security Inside series. The podcast is available at https://www.youtube.com/watch?v=3fBfS163oDg)

These competitions showcase real-world security issues by presenting security bugs on actual hardware, and my experiences with them have been amazing. They provide researchers a chance to tackle real-world problems and come up with innovative solutions to mitigate security risks.

CyberByte: Do you have any tips to pass along to other students on how to excel at these types of competitions?

Chowdhury: My advice is to become proficient in writing software and learn scripting. In order to succeed in these competitions, it is necessary to have the ability to prototype and implement ideas from papers and discussions. If competing on your own, strong software engineering skills are a minimum requirement. Additionally, it is important to have a mentor or guide with years of experience in these competitions who can teach you how to run existing tools and understand their limitations.

I was fortunate to receive mentorship and training from my manager and their group at TRDDC, which laid the foundation for my objective thinking and approach to problems. Moreover, my previous experience allowed me to familiarize myself with tools like KLEE (Symbolic test generator) and AFL (greybox fuzz testing tool for discovering security bugs). This helped me excel in these competitions. Although these tools have a steep learning curve, they can be learned quickly with proper guidance.

CyberByte: Based on your research, how does this machine learning and artificial intelligence technology aid in the design of more hack resistant systems? And, do you have any concerns about how hackers can use this technology?

Chowdhury: DARPA hosts a highly engaging competition in the field known as the Cyber Grand Challenge competition. This competition involves two teams, the RED team and the BLUE team, with the RED team tasked with finding and exploiting vulnerabilities in the system, and the BLUE team tasked with finding and fixing the vulnerability before the RED team can exploit it. With advancements in machine learning and AI, large language models have the ability to detect and repair bugs in code. It is important to remember, though, that professionals should not solely rely on the suggestions made by AI-based code assistants, particularly in the context of safety-critical applications. Users must manually verify any changes made to code.

As for potential use by hackers, it is always possible that cybercriminals can leverage AI systems to scan code and identify potential security weaknesses. Ultimately, it becomes a contest between two AI agents representing the RED and BLUE teams, and the better-trained AI wins.

CyberByte: What is your anticipated graduation date? And, do you have any plans for what type of career you'd like to pursue when you're done?

Chowdhury: My goal is to complete my thesis and receive my degree by the end of Summer 2023. I then intend to continue working on applying machine learning for chip design and developing new deep learning algorithms to solve complex optimization problems. During my last summer internship at Qualcomm, I did a presentation on my previous work in security testing using greybox fuzzing and it generated a lot of interest in developing an in-house framework. Ultimately, my career plans include working in industrial research and exploring the two areas of: 1) Machine learning for chip design and 2) Enhancing security testing for software and hardware through learning.

ALUMNI PROFILE:

DR. KEVIN GALLAGHER

DIFFERENT CONTINENT, SAME COMMITMENT TO "TECHNOLOGY AS A FORCE FOR SOCIAL CHANGE"

A hallmark of the professional career of NYU/CCS alumnus Dr. Kevin Gallagher has always been a commitment to using technology to support activism and protect individual privacy. During his tenure at Tandon, first as a master's student and then as a Ph.D. candidate, his research focused on anonymity networks and strategies to combat censorship, culminating in his dissertation work on "Measurement and Improvement of the Tor User Experience." At the same time, he trained individuals and at-risk communities on personal cybersecurity and surveillance self-defense, served as a core contributor to the Tor Project, and held a number of research and teaching assistant posts before becoming an adjunct professor at Tandon. Since completing his doctorate in 2019, Gallagher has moved to Portugal, where he continues his commitment to privacy and anonymity research, activism, and education as a faculty member, researcher, and nonprofit group founder.

CyberByte recently caught up with Gallagher to ask about teaching methods, the differences between the students he worked with at NYU and the ones he taught at Instituto Superior Técnico at Universidade de Lisboa (https://tecnico.ulisboa.pt/pt/), the status of cybersecurity awareness in Portugal, and his own current research initiatives.

CyberByte: Your website lists a number of different "job titles," so let's start by untangling your commitment to these various projects.

Gallagher: Up until February of 2023, I was an Invited Assistant Professor at Instituto Superior Técnico at Universidade de Lisboa (https://tecnico.ulisboa.pt/en/) and a researcher at Instituto de Engenharia de Sistemas e Computadores - Investigação e Desenvolvimento (INESC-ID). In Portugal, universities only do teaching, while research labs affiliated with the universities do research. It's kind of like if the Center for Cybersecurity in NYU was a separate legal entity from NYU. It's a confusing system, and one I'm still wrapping my head around. These labs tend to be linked to specific universities, so now that I'm a tenure track assistant professor at the Faculdade de Ciências e Tecnologia at Universidade NOVA de Lisboa (https://www.unl.pt/en/nova/nova), I'm working with a new research lab called NovaLincs (https://nova-lincs.di.fct.unl.pt/).

As I understand it, the reason research institutes are separate entities is because most universities are public, and faculty are viewed as public servants. There is a formal process for hiring faculty that includes posting public announcements of open positions and negotiating considerable layers of bureaucracy. Keeping research work separate means there is more flexibility in both hiring, and in the choice of topics for investigation.

As for the other titles, I am also the founder of PrivacyLx, a nonprofit organization that teaches the general public how to reclaim their privacy through education. And, I've been a Tor core contributor for a number of years. Both of these are volunteer positions.

CyberByte: You taught at NYU for a while before leaving for Portugal. How different is the classroom experience there from what you saw at Tandon?

Gallagher: For starters, what is considered teaching in Portugal is different.The paradigm of education here is called 'The Empty Vase,' which means the teacher pours knowledge into "empty" students. The professor's job is to present the lecture and then each class has a laboratory section that offers more hands-on help. These teaching lab sections tend to be taught by less-experienced faculty. At first, I taught the practical labs of the Highly Dependable Systems course, which largely focused on tactical Byzantine Fault Tolerances. At times, I felt more like a TA than a teacher.

I guess, in terms of differences, I should mention the language. Though graduate courses are taught in English, freshman classes are taught in Portuguese. I'll be teaching freshman classes this semester, so this will be new.

CyberByte: Have you noticed any differences in either student attitudes, quality of work, or openness to ideas in comparison with the students you worked with at NYU?

Gallagher: I mostly taught CyberFellows at NYU, individuals who had work experience and who perhaps were a bit older than traditional students. So there are obvious differences between the two groups. There is also a deference to authority here. I like being challenged by my students, but I haven't seen that here, except in a thesis setting. It should be noted that Portugal was a dictatorship till 1974. So, perhaps in a few years we'll see more of that push back in the average classroom.

CyberByte: Other than Highly Dependable Systems, what other classes have you been teaching?

Gallagher: I teach a new Ph.D. level course I developed called Fundamentals of Privacy and Anonymity. I have also taught both the lecture and lab segments of Advanced Topics in Parallel and

Distributed Computing. The latter class, which is a Ph.D. level course, allows students to rapidly bootstrap knowledge in the area of blockchain and be ready to perform research in this area, as block chain is currently a hot topic for grant funding here. The class also emphasizes important skills for academics, such as paper reviewing, presentations, and choosing research problems.

CyberByte: What are some of your recent research projects?

Gallagher: I have continued my research initiatives with the Tor project and recently submitted a paper on building some robustness into Tor to avoid traffic confirmation attacks. In these attacks, the hacker controls or observes the relays on both ends of a Tor circuit and then, by comparing traffic timing, volume, or other characteristics, can conclude that the two relays are indeed on the same circuit. I also just submitted a paper entitled, "Studying the Online Deepfake Creation Community," which was coauthored by several former Tandon colleagues, including Drs. Damon McCoy and Rachel Greenstadt. The paper offers an in-depth look at "Mr. Deepfakes," a community for the creation of "nonconsensual deepfakes porn," or sexually explicit videos and images featuring famous people. In particular, we were interested in tracking the source of deepfake technology, and determining the "bleed" between those just accessing the site to seek information about it and those actually seeking its products.

Lastly, I'm continuing a project on re-thinking cybersecurity primitives. Cybersecurity has its origin in the military, and so its primitives typically exhibit a very top-down hierarchical structure. This structure does not work well for more decentralized organizations, such as trade unions, activist groups, or worker cooperatives. Instead, we want to promote the idea of horizontal security, or security techniques and technologies that utilize democratic participation for security decision-making. I've already published one paper on this topic, again in collaboration with some Tandon colleagues (Dr. Santiago Torres-Arias, who is now at Purdue, and Dr. Nasir Memon. To learn more, read the paper at https://dl.acm.org/doi/pdf/10.1145/3498891.3498903). Our next steps include identifying what changes are needed in cybersecurity concepts and technologies to facilitate horizontal security. We then plan to use a solution similar to the one proposed in the original paper to address a particular attack threat model endemic to the organization of the Portuguese Parliament. Portugal has multiple political parties, but they share a parliamentary infrastructure that is managed by an administrative team with "superuser" powers. At the moment, a given administrator could use these "superuser" powers to spy on other parties or, worse, delete or modify information. Our solution calls for an administrative council that would impose a system of checks and balances for administrators. Any attempt to perform an action that requires superuser influence, would need approval from a council of administrators.

CyberByte: I am curious how Portugal compares with the U.S. in attitudes towards cybersecurity. How aware are people about cyber threats?

Gallagher: Take the state of the art in the U.S. and go back about 10 to 15 years and that's the status here. There is also a large disconnect between the government and the industry/academic sectors when it comes to these issues. Awareness of the threat has reached critical mass, but the government doesn't know how to respond. An aging Parliament is probably one reason for this disconnect.

CyberByte: Lastly. I'd like to hear a bit more about your work with PrivacyLx. Can you talk a bit more about the goals of the group? And what has been the response to your workshops and programs?

Gallagher: As stated on our website, PrivacyLx is a nonprofit organization (https://privacylx.org/) that focuses on the defense of privacy and digital security as fundamental rights for a free society through education, research and development of tools for their protection. It was founded in 2018, when I was still at NYU. One of our programs is what we call Privacy Cafe, where anyone can bring in a laptop, smartphone or tablet and our volunteers show them how to protect their data and devices. Unfortunately, Covid really hurt us. We found that cyber events did not work for this audience, so it all kind of stopped for a while. We've begun programming again though, so hopefully momentum will return.

CCS Co-chair Dr. Ramesh Karri and Dr. Nikhil Gupta, Hack3D competition lead, outside the entrance to CSAW'22.

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)

16
Partner Organizations

1,420
Qualifying Teams

9
Sponsors

128
Team Finalists

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.

Team ROAR from Clemson University delivering their first place winning presentation in the Hack3D competition.
(L to R) Shamanth Manjunath, Ethan Wescoat, Flanagan Waldherr

PROTECTING BLOCKCHAIN, TIME SERVERS, AND MORE

At the CSAW'22 US-Canada site, the program also featured a series of talks about cyber risks and prevention in a number of emerging sectors. Stephen Tong, who has been at CSAW many times as a member of the Perfect Blue Capture the Flag team, started things off with a discussion of strategies for protecting smart contracts.Tong is a co-founder of Zellic, which specializes in blockchain security. Also, representing the financial sector was Ajoy Kumar, Managing Director and CISO with DTCC, who focused much of his talk on emerging opportunities in the cybersecurity field.

Two CSAW speakers, Ali Naqvi, a manager with Consolidated Edison's Cybersecurity Operations Center, and Abhishek Ramchandran, Penetration Testing Team Lead at Siemens, spoke about issues in critical infrastructure, a category that includes pipelines, water treatment facilities, chemical plants and nuclear reactors. Naqvi pointed out some major characteristics of what he called "operational technology security" that need to be accounted for in addressing security problems in this sector. These include protocols that may or may not be standardized, a limited number of defensive tools, and increasingly stringent regulations. Ramchandran of Siemens focused on how obsolete components in a facility can be hacked and used as a way to leverage access into critical infrastructure systems.

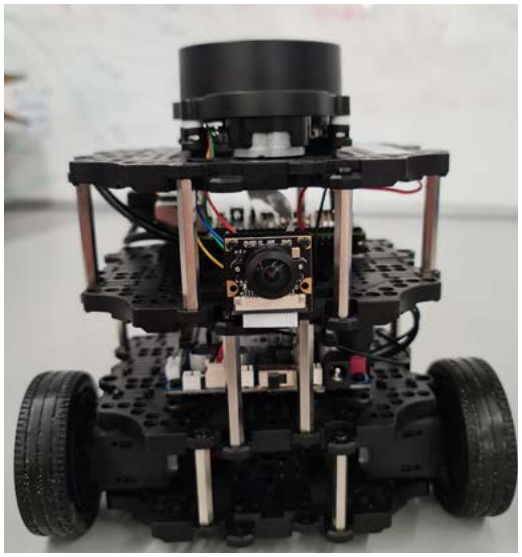
Kurt Rosenfeld of Google presenting as part of the opening day talks at CSAW US-Canada

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.



Robot devices used in the Hack my Robot competition

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."

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

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 Ayllon, 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 will ensuring that all criteria are "manageable yet challenging for the participant teams."

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.

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 Mammone, Davide Luca Merli

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

- **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, Nimish 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

CCS NEWS

GARG AND CAPPOS TURN SUPERHEROES AS TWO OF TANDON'S "AGENTS OF OPTIMISM"

In December, 2022, NYU Tandon released a unique marketing campaign to promote the groundbreaking work of its engineering and science faculty. With a cheeky nod to several superhero franchises, it introduced 10 faculty members from a number of disciplines, along with Tandon Dean Jelena Kovačević, as "Agents of Optimism." The initial trailer that dropped in early December on YouTube was followed by individual short films on each of the "agents," along with a downloadable comic book.

The Center for Cybersecurity is represented in the superhero collective by Dr. Justin Cappos, an associate professor of computer science and engineering, and Dr. Siddharth Garg, Institute associate professor of electrical and computer engineering. Tagged as the "Hacker Halter" and the "Digital Defender," respectively, the campaign touts their research accomplishments in defending systems and protecting digital infrastructure from attacks.

The campaign, which was mentioned in a recent LinkedIn article (https://www.linkedin.com/pulse/7-sparks-he-marketing-excellence-inspired-us-2022-jim-tudor/?trackingId=cn7mYL4XRq2KlhX9CS9xDA%3D%3D) as a "spark of inspiration" among higher education marketing programs, comes in the wake of an announcement by NYU on November 30 of a $1 billion investment in its engineering programs that included the purchase of 3 Metrotech (https://engineering.nyu.edu/about/nyu-investing-1-billion-tandon). In stating its plans for the new funds, the school affirms a special commitment to support research efforts in securing wireless infrastructures and supply chains, data science, and sustainability. These choices are echoed in the selection of the "Agents of Optimism" team.

To see the trailer and each of the individual superhero films, or to download the comic book, go to https://engineering.nyu.edu/tandon-agents-optimism.

NYU/KAIST BEGIN NEW GLOBAL PARTNERSHIP

Back in September of 2022, New York University and the Korea Advanced Institute of Science and Technology (KAIST) announced a historic partnership that would, among other things, "lay the groundwork for a joint presence in New York City—KAIST's first campus in the United States." On February 23 and 24, representatives from both institutions gathered at 370 Jay Street for their first joint workshop. Attendees focused on mapping out common areas of interest and expertise, and discussed special initiatives in four technical areas.

The first day was devoted to discussions on three of these common areas: software and system security, privacy-preserving computing, and human aspects of security (e.g. biometrics, mis/disinformation, privacy of IoT, wireless, legal). A fourth topic, "the intersection of NextG Wireless/Robotics and CyberSecurity," was explored on the second morning. Each topic was addressed in a session organized by one representative from each institution. On NYU's side, that included several faculty and staff from the Abu Dhabi campus, as well as the New York campus.

The workshop ended with a roundtable discussion that looked to "identify synergies, collaborations, and promotion." Out of these discussions came a full list of potential participants across all the institutions involved, a list of possible funding sources for the work ahead, and planning for several new educational initiatives. The latter would include an undergraduate minor in cybersecurity that would be awarded by KAIST based on NYU courses, a "Build Your Own Masters" MA program with a privacy engineering specialization, and a dual degree Ph.D. The partnership will eventually also include outreach activities that build on existing programs like CSAW, and leverage industry contacts, such as the Cyber Fellows Advisory Council and the Cybersecurity Lecture.

For more information on the partnership, go to https://www.nyu.edu/research/nyu-kaist.html.

Representatives of NYU and KAIST pose with incoming NYU President Dr. Linda G. Mills (at center)

CFD/GLOBAL WITNESS STUDY FINDS FACEBOOK ACCEPTED THREATENING ADS

In a test of how well social media outlets enforce their own policies about harmful content in advertising, Facebook clearly fell short during the US midterm elections, according to a study conducted by Global Witness (https://www.globalwitness.org/en/) and NYU's Cybersecurity for Democracy (C4D) (https://cybersecurityfordemocracy.org/). The study found that Facebook either failed to detect, or just ignored, death threats against election workers contained in a series of ads submitted to the company.

According to a report jointly released by both organizations on December 1, 2022 (https://cybersecurityfordemocracy.org/post-midterms-election-disinfo), the researchers submitted advertisements that included threats against election workers. Though the ads were fakes, the types of death threats made had actually been reported within the media. A total of 20 such ads were prepared—10 each in both English and Spanish—and submitted to Facebook, YouTube, and TikTok. In all cases, the submissions violated the platforms' stated ad policies, and "the death threats were chillingly clear in their language."

The ads were submitted to the three social media sites on the day of or the day before the 2022 US midterm elections. The results could not have been more different. "TikTok and YouTube suspended our accounts for violating their policies," the report observes, while Facebook "approved 9 of the 10 English-language death threats for publication and 6 of the 10 Spanish-language death threats. Our account was not closed down despite a handful of ads having been identified as violating their policies." When asked about these findings, a spokesperson for Meta, Facebook's parent company, responded: "This is a small sample of ads that are not representative of what people see on our platforms. Content that incites violence against election workers or anyone else has no place on our apps and recent reporting has made clear that Meta's ability to deal with these issues effectively exceeds that of other platforms. We remain committed to continuing to improve our systems." The report concludes with a list of specific actions the research team feels social media platforms in general, and Facebook in particular, should take to stop the proliferation of threatening ads.

More recently, Cybersecurity for Democracy, a project of the NYU Center for Cybersecurity, released a report on Facebook's response to the January 6, 2021 attack on the U.S. Capitol. "Understanding the (In)Effectiveness of Content Moderation: A Case Study of Facebook in the Context of the U.S. Capitol Riot," can be accessed at https://cybersecurityfordemocracy.cdn.prismic.io/cybersecurityfordemocracy/d27c54b5-d05e-40fc-81c3-df89677625f8_jan6-arxiv.pdf.

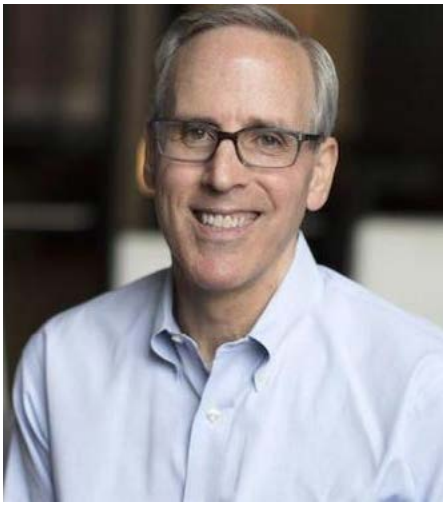
CISO CERTIFICATE PROGRAM HELPING TO FILL IMPORTANT GAP IN CORPORATE LEADERSHIP

As organizations wake up to the growing importance of defending its systems and information from attack, the need for executives with a strong grounding in the fundamental principles of cybersecurity has never been greater. To fill this void, NYU Tandon has launched a new certificate course to prepare senior professionals to serve as Chief Information Security Officers (CISOs). Developed in collaboration with Emeritus, a company that partners with major universities worldwide to offer short courses and professional certificate programs, it welcomed its first cohort in March of 2022.

The nine-month program is built around an 18 week core curriculum. According to Allie Krech, Assistant Director of Executive Education for NYU Tandon, during this core period, "one module is released per week, and the time commitment for each is about 3-5 hours per week." Over the rest of the program, participants engage in virtual peer-networking sessions, as well as live sessions with faculty and other industry leaders. Participants can also choose from a number of elective courses on topics, including threat intelligence and cybersecurity analytics, data science and machine learning in cybersecurity, and network security.

Students complete a variety of optional and mandated assignments of which perhaps the most valuable is what Ms. Krech describes as "an overarching capstone assignment to complete a CISO playbook based on exercises conducted each week." More than just an exercise, Kreich describes the playbook as "a takeaway, something tangible they can use in the workplace."

The program faculty includes a number of distinguished leaders in the cybersecurity field, two of whom have ties to the NYU Center for Cybersecurity. Jim Routh, pictured at right, serves as the program's faculty director. Routh is also a member of the NYU Cyber Fellows Advisory Council (https://engineering.nyu.edu/advisory-council/jim-routh). He brings with him practical experience as a CISO or CSO for a number of institutions, including MassMutual, Aetna, and JP Morgan Chase, to name a few. Dr. Edward Amoroso, Chief Executive Officer for TAG Cyber LLC and a Distinguished Research Professor with the Center for Cybersecurity, is also on the faculty.



At the time this article was written, the CISO certificate program was preparing to welcome its third cohort of students. Ms. Krech observed that though all candidates for the program must have at least 10 years of work experience, there is still a good deal of diversity in terms of background and previous education. "We have had participants from such industry sectors as biotechnology, pharmaceuticals, and education, some with advanced degrees and some without." She also noted that "candidates for the program self-select pretty well. Most candidates that are turned away tend to not be from the information security space and lack the background in cybersecurity or information security." Thus, most candidates that fit the criteria do get to participate.

For more information on the CISO certificate program, go to https://engineering.nyu.edu/academics/programs/chief-information-security-officer-program.

DTCC PARTNERS WITH NYU TANDON TO ADVANCE RESILIENCY CONCEPTS IN TEACHING AND RESEARCH

On September 7, the NYU Tandon School of Engineering and The Depository Trust & Clearing Corporation (DTCC) announced a new five-year partnership to advance the work of the NYU Center for Cybersecurity. A primary goal of the partnership is to expand the concept of resiliency in CCS research and educational offerings.

According to an announcement published by DTCC, a firm that "automates, centralizes, standardizes, and streamlines processes in the capital markets," the partnership aims to "expand the pool of Ph.D. students researching cybersecurity and resiliency at NYU Tandon." It will also assist in developing resiliency curricula at both the undergraduate and graduate levels.

In acknowledging the partnership, Dean Jelena Kovačević of NYU Tandon noted that it will allow students, "to stay a step ahead of threats as they become more sophisticated. With its immense pool of expertise, DTCC will accelerate development of talent in both research and academics." Lynn Bishop, Managing Director and Chief Information Officer at DTCC adds, that the partnership will enable DTCC "to share its expertise in IT with tomorrow's cybersecurity and resiliency professionals and provide them with real-world knowledge and scenarios based on deep expertise and our pioneering work using new technologies."

FAUXPILOT: AI-ASSISTED CODE GENERATION WITH NO STRINGS ATTACHED

Want the benefit of an AI-assisted code generation program like GitHub Copilot, (https://github.com/features/copilot) but don't want to be tethered to the Microsoft universe? Dr. Brendan Dolan-Gavitt, an associate professor of computer science and engineering at Tandon, has developed an alternative. In the summer of 2022, he introduced the cheekily-named FauxPilot (https://github.com/fauxpilot/fauxpilot/blob/main/README.md).

The primary goal of the new program is to eliminate the need to share information with third parties, and by doing so, avoid potential copyright issues and other complications.

"There are people who have privacy concerns, or maybe, in the case of work, some corporate policies that prevent them from sending their code to a third-party," Dolan-Gavitt told Thomas Claburn in an article in *The Register*. "FauxPilot addresses these concerns and that definitely is helped by being able to run it locally."

By "running locally," Dolan-Gavitt is referring to FauxPilot's ability to run AI assistance software on "premise." This differs from GitHub Copilot, which through telemetry can end up sending some data back to GitHub, which is owned by Microsoft. FauxPilot also reduces, if not totally eliminates licensing concerns, because, unlike Copilot, it does not utilize OpenAI Codex. As explained in the article, this "natural language-to-code system" was "trained on 'billions of lines of public code' in GitHub repositories (see https://github.blog/2021-06-30-github-copilot-research-recitation/).Thus, it's possible the system incorporates copyrighted data from other sources that could expose users to infringement threats."

The full article, which was originally published on August 6, 2022, can be found at https://www.theregister.com/2022/08/06/fauxpilot_github_copilot/?__s=p54njaazgqic1gqfruk3.

EVENTS

CCS LAW FACULTY CONTRIBUTE TO PANEL ON CYBERSECURITY AND INFRASTRUCTURE

Last fall, the NYU Law School hosted a conference entitled "Structuring Enforcement to Deter Misconduct and Induce Disclosure." The purpose of the day-long session was to inform attendees about "the current state of law, regulation and policy," particularly the evolution of "corporate enforcement policy, and how it can be adjusted to deter misconduct and induce self-disclosure by companies."The conference was also designed to deepen "understanding of the impacts of corporate self-disclosure on society, enforcement and all stakeholders."

The day was divided into four distinct topical sessions, with the last two "focusing on issues concerning cybersecurity regulation, compliance and enforcement." Specifically, the session addressed self disclosure activities by the SEC regarding public company reporting of material cyber risks and incidents, and a separate initiative regarding self-disclosure of cybersecurity incidents.

Professor Randal Milch moderates panel on Cybersecurity and Infrastructure

Judith Germano replies to a question.

The closing panel of the day was entitled "Cybersecurity and Infrastructure" and examined issues of regulation and disclosure as applied to the increasingly vulnerable area of critical infrastructure. The panel was moderated by Randal Milch, a Professor of Practice at the Law School and co-chair of the Center for Cybersecurity. CCS was also represented by Distinguished Fellow Judith Germano, who served as one of the panelists. Other participants were:

- Leonard Bailey, Special Counsel for National Security, Computer Crime & Intellectual Property Section, US Department of Justice
- Ann Fairchild, Senior Vice President and General Counsel, Siemens Corporation
- Kevin Morley, Manager of Federal Relations, American Water Works Association

The fall conference is part of an ongoing program sponsored by the law school's Program on Corporate Compliance and Enforcement.

AWARDS AND HONORS

LARX RESEARCHERS HONORED AT FALL CONFERENCES

Congratulations to Dr. Quanyan Zhu and his Laboratory for Agile and Resilient Complex Systems which brought back honors from two fall conferences. First, Zhu and recent Ph.D. graduate Dr. Linan Huang (photo right), were named recipients of the Koopman Prize, awarded by the Institute for Operations Research and the Management Sciences (https://www.informs.org/Recognizing-Excellence/Community-Prizes/Military-and-Security-Society/Koopman-Prize). The award recognizes the "outstanding publication in military operations research of the previous year." Huang and Zhu were selected for their paper "Duplicity Games for Deception Design With an Application to Insider Threat Mitigation," which develops "a theoretic design framework to deceive and deter attackers by strategically manipulating their perceptions of information and cost."

Later that month, Ph.D. candidate Yunian Pan (photo left) took the best paper award at the 13th International Conference on Decision and Game Theory for Security Conference, held in Pittsburgh, PA, from October 26-28. Pan received the recognition for his work entitled "On Poisoned Wardrop Equilibrium in Congestion Games," which "exposes the vulnerability of the increasingly interconnected traffic networks against the informational attack vectors."

NYU | TANDON

CENTER FOR
CYBERSECURITY

cyber.nyu.edu