NYU | TANDON SCHOOL OF ENGINEERING

NYU CENTER FOR CYBERSECURITY

CYBERBYTE

SPRING 2022

IN THIS ISSUE

Protecting the weakest links: How CCS researchers are defending the software/hardware supply chain

When agencies of the U.S. government and several private technology firms detected the Sunburst virus at the end of 2020, it affirmed a long overlooked reality that security measures cannot be limited to protecting just the finished product. As the dust began to settle in early 2021, "supply chain security" became a priority in every industrial sector, from chip manufacturing, to power plants, to automobiles.

Researchers at the Center for Cybersecurity have been working on supply chain security issues long before such demands hit the headlines. This puts CCS in a unique position to address both industry fears and government regulations, such as those enumerated in both Executive Order #14028, which mandates modernizing cybersecurity defenses, and the comprehensive Executive Order #14017, which lays out guidelines for more resilient supply chains in a number of industry sectors.

Given the strategic importance of supply chain technology at this moment in time, CyberByte has chosen it as the debut topic of our new "Research Focus" feature. Beginning on pg. 3, you will be able to read some short updates about how CCS research teams are dealing with supply chain security issues in cyberphysical infrastructure, chip manufacturing, and more. We will cap off the section with a Faculty Profile featuring Dr. Justin Cappos, associate professor of computer science and engineering and a researcher who has spent a good portion of his professional career seeking practical solutions for security gaps, including those present in software supply chains.

Dr. Quanyan Zhu
Editor-In-Chief, Cyberbyte

OUR TEAM

Editor in Chief
Quanyan Zhu

Editorial Copy Writer
Lois De Long

Production Manager
Emerald Knox

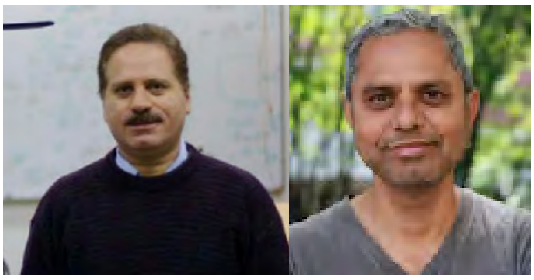
RESEARCH FOCUS: Defending the Software/ Hardware Supply Chain

The challenges in securing the supply chain of any project in any industry can be traced to a few common problems: multiple production steps involving numerous suppliers and manufacturers, a lack of shared standards for specifying materials, and little or no verification of what was done at each step and by whom. With software now commonly created by developers on different continents, and chip manufacturing largely limited to plants in other countries that may or may not monitor products for possible tampering, perhaps no ecosystem is in greater need of standardized supply chain protection practices than the computing industry.

Here are a few of the supply chain-related research initiatives underway at the Center for Cybersecurity.

DETECTION

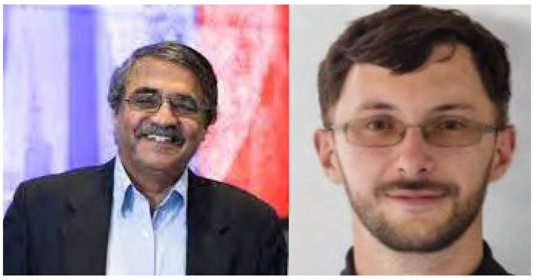
Though there are advantages to outsourcing the manufacture of integrated circuits, it does open the possibility that newly fabricated chips can carry with them deliberate flaws known as Trojans. To resolve this issue, and thus eliminate one source of risk to the supply chain, CCS co-chair Dr. Ramesh Karri (at right in photo) is collaborating on a novel detection technique that creates algorithms to detect Trojans based on the short term aging phenomena in transistors. With funding from the Office of Naval Research as part of its Defense University Research Instrumentation Program (DURIP), Karri and Dr. Farshad Khorrami, a Professor of Electrical and Computer Engineering at Tandon, are building a testbed that can provide access to physical integrated circuits with both Trojan-free and infected variants of circuits. The testbed would also include a fast switching programmable power supply for precise application of supply voltage changes to the IC's being tested.



The research team also includes Jörg Henkel and Hussam Amrouch of the Computer Science Department of the Karlsruhe Institute of Technology (KIT), Karlsruhe, Germany, and Tandon research scientist Prashanth Krishnamurthy. Looking forward, the team believes that the testbed could be a vital resource in the physical validation of hardware Trojan detection techniques.

DISTORTION PREVENTION

One supply chain threat that is particularly insidious is the use of digital manipulation to alter images. As noted by Dr. Nasir Memon (at left in photo), co-founder of the Center for Cybersecurity in an article published in IEEE Transmitter this fall, “the rise of sophisticated digital technologies that can alter visual and aural inputs in a way that can seamlessly change their meaning has caused tasks as simple as declaring an image ‘real’ or a video ‘accurate’ to become surprisingly difficult.” (https://transmitter.ieee.org/why-seeing-must-be-believing-ai-computational-imaging-and-the-battle-against-deepfakes/) As a defensive strategy against this threat, Memon began working with NYU Tandon colleague Dr. Pawel Korus two years ago to design a camera pipeline that replaced the traditional photo development pipeline with a neural network trained to jointly optimize for high-fidelity photo rendering and reliable provenance analysis. Around the same time, the industry as a whole became actively engaged in “providing provenance and history for digital media” with the formation of the Coalition for Content Provenance and Authenticity (C2PA). (https://c2pa.org/) Now a Joint Development Foundation project, C2PA provides an open technical standard to enable publishers, creators, and consumers the ability to trace the origin of different types of media.



Meanwhile, Memon and Korus continue to build on their initial work with the creation of an open source library to support modeling and optimization of photo acquisition and distribution pipelines at https://github.com/pkorus/neural-imaging, and are getting ready to publish a new variation on their camera pipeline solution later this year.

QUALITY ASSURANCE

In addition to security concerns, protecting the supply chain can also mean ensuring the uniform quality of critical components outsourced to multiple suppliers. Unfortunately, the increased accessibility of digital manufacturing systems puts these tools in the hands of people that may not really understand how to use them. This opens the possibility for great inconsistencies in product quality.

A cross-disciplinary team led by two CCS researchers, Dr. Nikhil Gupta from the Mechanical and Aerospace Engineering Department and Dr. Ramesh Karri recently conducted two studies to assess quality in parts produced via digital manufacturing. Working with Dr. Hammond Pearce, a post-doctoral researcher in the Center for Cybersecurity (at left in photo), and Gary Mac, a PhD researcher in Tandon's Department of Mechanical and Aerospace Engineering (MAE), the first study (go to https://onlinelibrary.wiley.com/doi/full/10.1002/mds3.10153) looked at a 3D printed metal part used in maxillofacial surgeries. On-demand 3D printing services are advantageous to doctors because medical devices often require customization, and being able to print parts could allow for faster response in emergency situations. However, the study found that the dimensional variations in the printed parts can be as high as 12%. A second study (go to https://www.sciencedirect.com/science/article/pii/S2352340921005709) monitored product quality of a standard test artifact as manufactured using multiple 3D printing technologies. It found that the quality of a printed part is dependent on the optimization of the 3D printers' operating parameters, and requires an operator with a strong background in the technology.

FINANCIAL INCENTIVES AS DEFENSIVE MECHANISMS

Public Electric Vehicle Charging Stations (EVCSs) are especially vulnerable to load-altering cyberattacks because they can be accessed by the public and are not continuously monitored by electric power utilities. To address this infrastructure risk, CCS and NYU Tandon School of Engineering researchers have proposed a unique strategy: cyber insurance that can hedge the financial losses such attacks can cause, while serving as an incentive to promote compliance with security standards and adopt best practices. In a paper published in December of 2021 (https://arxiv.org/pdf/2107.03954.pdf), Samrat Acharya (at left in photo), a Ph.D. student, working with Dr. Ramesh Karri, Dr. Yury Dvorkin, Goddard Junior Faculty Fellow in the Department of Electrical and Computer Engineering (at right in photo), and several others, propose a "data-driven cyber insurance design model for public EVCs" that utilizes domain-specific risk modeling techniques. Their research found that "risk assessment is crucial for designing insurance premiums," and that "the premium increases in proportion to the loss coverage offered for the EVCSs." By demonstrating that insurance premiums can be reduced by deploying state-of-the-art defense mechanisms, it serves as a financial incentive to abide by regulations and standards.

FACULTY PROFILE: DR. JUSTIN CAPPOS

Minding the Gaps in Software Security

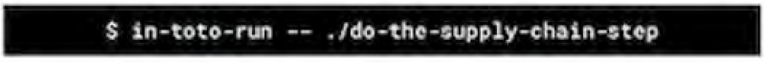
Not every software researcher needed the wake-up call of the SolarWinds / Sunburst attack to initiate solutions for securing supply chains. Dr. Justin Cappos of NYU's Center for Cybersecurity estimates that about half of the research projects he has led over the past two decades have addressed security gaps in the software supply chain. "It's an area that is somewhat overlooked in academia," he posited in a recent interview, adding the observation that "companies don't compete over who has the best software."

Yet, by focusing on "the path between the repository and the user," he has led projects that have repaired vulnerabilities in package managers and strengthened software update systems to ensure resilience, even when compromised by nation state actors. So, it's not so surprising that, in tandem with a colleague at the New Jersey Institute of Technology and his former Ph.D. student Santiago Torres-Arias, he also created a framework which he feels could become "the de facto standard for software supply chains." That framework, called "in-toto," Latin for "as a whole," can ensure the integrity of a software product from initiation to end-user installation. It does so, according to its website (https://in-toto.io) by "making it transparent to the user what steps were performed, by whom, and in what order."

In some ways, the introduction of in-toto is part of a natural evolution through the software development chain for Cappos, now an associate professor of computer science and engineering at NYU Tandon and the director of its Secure Systems Laboratory (https://www.ssl.engineering.edu).

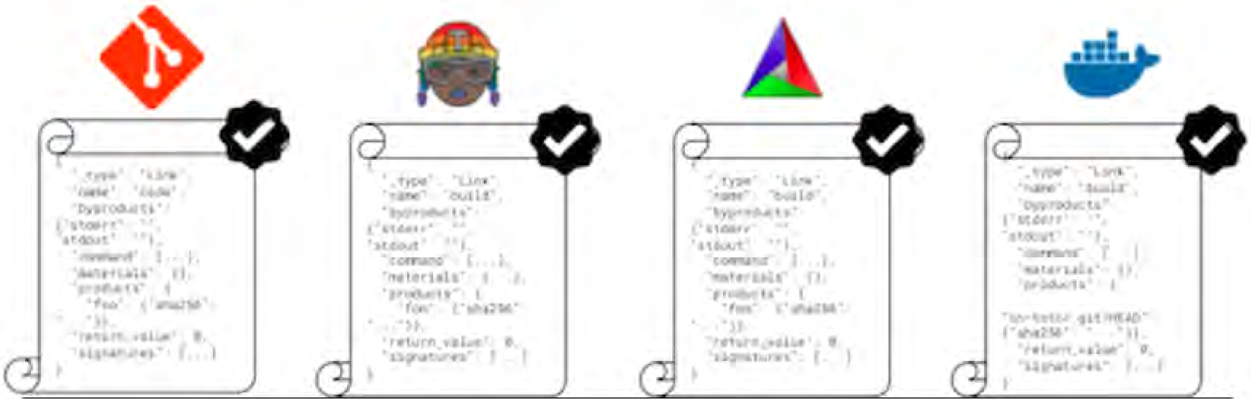
His initial work as a doctoral candidate at the University of Arizona identified the use of mirrors as a vulnerability in download processes. As a solution, he introduced a package downloader called Stork that protected virtual machines running over distributed networks. Still used today In many Linux package managers, the work represented the first o f many security g aps he would identify and rectify.

Another of these identified gaps was having no way to determine if a file or image had been changed or modified during the m ulti-step development process. "I had a pretty well-formed idea about dealing with this problem," he recalled. "And then I met Dr. Reza Curtmola, of the New Jersey Institute of Technology, who had already written a paper about software repository security. We wrote a grant together and the project was underway." Torres-Arias, who had been investigating password security issues, came on board as the lead developer and designer for the project. Cappos gives Torres-Arias credit for "making its implementations practical." Since then, in-toto has been adopted or integrated into several major open source software projects, including those hosted by the Cloud Native Computing Foundation, a part of the Linux Foundation. It's also worth noting that SolarWinds, the company that inadvertently spread the Sunburst malware, adopted in-toto and described its integration in a presentation at Supply Chain Security Con (https://static.sched.com/hosted_files/supplychainsecurityconna21/df/SupplyChainCon-TrevorRosen-Keynote.pdf).



```
$ in-toto-run -- ./do-the-supply-chain-step
```

An illustration of in-toto attestations for the four primary steps in software development: code, test, build, and package.



At the heart of its operations, in-toto works by providing signed attestations for each stage of development, adding accountability and, should a vulnerability be found, a clear way to track its source. But, what if the flaw was introduced in an earlier stage of development, maybe as far back as the GitHub repository in which it was initially designed? In answering this question, Cappos closed yet another gap—securing the version control programs where software is created and modified. "Almost all software is made using git repositories. Yet there are gaps in the protection that git provides even if developers sign every commit." This led Cappos and his collaborators to design a new signing scheme for git, which was adopted in 2017.

Cappos is also working on the broader problem of securing data other than software. "There is no secure way to protect the broader classes of digital documents, such as legal records, legislation, or other living documents." Cappos is currently teamed up with researchers from the Open Law Platform on a project called The Archive Framework (TAF) that can identify attempted attacks along branches in git and cancel malicious updates and commits. The project uses elements of The Update Framework, a Cappos-led project that has previously been used to secure targets as diverse as software repositories and automobile computing units.

In addition to his supply chain work, Cappos is currently engaged in building a decentralized content distribution network (CDN), and on resolving issues in software isolation. "I enjoy working on diverse and interesting problems in computing wherever I see them," says Cappos. For the past year and half he has been working and teaching from NYU's Shanghai campus, which has enabled him to develop some new research partnerships and collaborations with industry. "Working in a new environment has enabled me to talk with different collaborators in fields like economics and manufacturing, leading to working on new problems from different perspectives," explains Cappos.

A willingness to explore different perspectives has also made it possible for Cappos to work comfortably between the academic and industrial sectors. As a result, he may be one of the few academic researchers to ever walk into a conference meeting room and see an ice sculpture in the shape of his TUF project logo. (photo left). "Thanks to the Cloud Native Computing Foundation, TUF has its own fashion line, with T-shirts, hoodies, socks, and even masks available for users and other fans (https://store.cncf.io/collections/tuf)," he reports. "These are some of the ancillary benefits of working with industry, and honestly, it can be a lot of fun." To Cappos, this is just one example of how academic work can have an impact on real-world projects, no matter how small it may seem. His practical mindset has also led to numerous requests to serve as an expert commentator on issues of cybersecurity and privacy for local, national, and international media, most recently in an article on CNET about emerging threats to cybersecurity in 2022 (https://www.cnet.com/tech/services-and-software/2022-shaping-up-to-be-an-epic-year-in-the-fight-to-protect-data/).

Looking ahead to what might come of the current focus on software supply chain security, Cappos tempers his optimism with some concern. "It's important that in a rush to do 'something,' that what is done is 'the right thing.' The worst outcome would be a bunch of people doing a bunch of bad solutions. I hope we are trending toward positive outcomes."

Ph.D. PROFILE: RASIKA BHALERAO

Assessing the Negative Impact of Positive Intentions

When is offering help not such a good thing? When the delivery of that help is wrapped in broad and often patronizing assumptions, or is outright harmful. Rasika Bhalerao, a fifth year Ph.D. candidate in Tandon's Computer Science and Engineering Department, drew the above conclusion after completing a study of sex industry workers (including survivors of trafficking) and the manner in which nonprofit groups seek to assist them. What she found was an ingrained, but incorrect, assumption that most sex industry workers are either trafficked or otherwise coerced to engage in sex for money. This assumption has fueled extensive proactive outreach initiatives to the sex industry by non-governmental agencies (NGOs), often in collaboration with religious and law enforcement agencies. By treating all sex industry workers as victims and exposing them to law enforcement, mass proactive outreach can actually make it harder for those individuals who truly need assistance, and often actively do harm.

Bhalerao, speaking at the CCS Ph.D. Research Lightning Talks on November 19, explained that there is a great deal of diversity among sex industry workers in terms of how much autonomy and control they have over their working conditions. Yet, the current efforts of groups reaching out to these individuals characterize the majority of sex industry workers as lacking agency, which leads to "organizations' misunderstanding of the ideal beneficiaries of unsolicited outreach messages." Organizations are also often unaware of the huge fear of law enforcement in the sex industry. "Proactive outreach messaging puts the recipients at risk of being exposed," Bhalerao explains, adding, "the risk of being 'outed' as a sex industry worker to friends, family, or anybody else is often top-of-mind for sex industry workers but not to those sending the outreach messages."

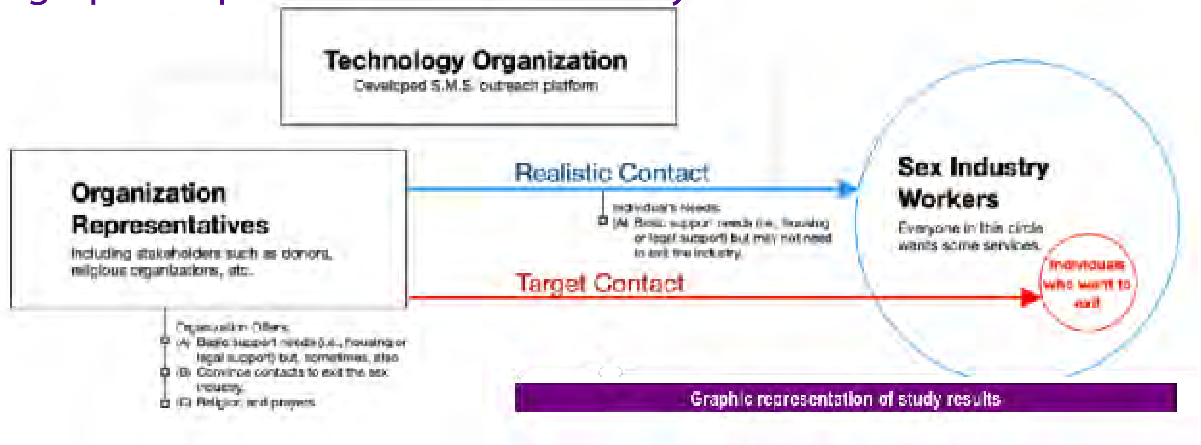
According to Bhalerao's study, while most sex industry workers report needing resources at some point in their life (such as legal or financial assistance, or health insurance), most do not want help "exiting" the sex industry. This unfortunate stereotype has been intensified by a number of false theories and fake news around the issue of trafficking. Bhalerao notes that, "there is a conspiracy theory that sex trafficking increases around the Superbowl, and that postings about it in gas stations and public restrooms will curb it." She also points to what she calls a "trafficking panic," often assisted by well-meaning promotion of the issue by actors and celebrities, which adds a sense of urgency that "ending the sex trade" is necessary or even possible, and exacerbates the stigma of the industry.

While a study of this nature may sound more like work for a social scientist rather than a computer scientist, Bhalerao points outs that anti-trafficking outreach relies heavily on computer technology, everything from scraping online sex ads to extract phone numbers, to the development of "hundreds of technological interventions designed to combat sex trafficking." A paper she co-authored on this topic lists several examples, including Memex (https://www.darpa.mil/program/memex), developed by the Defense Advanced Research Projects Agency, which indexes "forums, chats, advertisements, job postings, and hidden services" related to the sex industry in an effort to identify human trafficking online. Understanding the context, risks, and needs of the population affected should be key to the development of any technology.

Indeed, Bhalerao notes that her study evolved out of an initial request for assistance from an organization that was building a platform to perform mass outreach to the sex industry. The platform builders observed that they were not receiving many responses to their sex industry outreach and thought this meant the appeala were going to spam recipients, or fake phone numbers posing as sex industry workers. Bhalerao conducted a series of interviews with 24 sex industry workers (including survivors of trafficking), 17 representatives of organizations that aim to help sex industry workers, and 6 individuals involved in developing the outreach platform. Based on those conversations it was clear that the problem was how the appeals were written and sent. In addition to the overall patronizing tone of these messages, Bhalerao noted they were often accompanied by explicitly religious messages and lacked awareness of sex industry workers' fear of being "outed" or referred to law enforcement.

The study results, summarized in the graphic below, offer some practical advice for those building platforms for this type of work. First and foremost, it is better to let those truly needing assistance come to the organization rather than the organization bombarding all sex industry workers with materials they did not request. Bhalerao recommends that groups that insist on performing proactive outreach could post on the websites sex industry workers go to for jobs. "Listing services, posting phone numbers for 24-hour hotlines, or providing testimonials from others who have used these services acknowledges the agency of sex industry workers and gives them the chance to reach out if they choose to," she says.

A graphic representation of the study results


Technology Organization
Developed S.M.S. outreach platform
Organization Representatives
Including stakeholders such as donors, religious organizations, etc.
Realistic Contact
Individual's Needs:
(A) Basic support needs (i.e., housing or legal support) but may not need to exit the industry.
Target Contact
Sex Industry Workers
Everyone in this circle wants some services.
Individuals who want to exit
Organization Offers:
(A) Basic support needs (i.e., housing or legal support) but, sometimes, also
(B) Convince contacts to exit the sex industry.
(C) Religion and prayers
Graphic representation of study results

Bhalerao, who did her undergraduate work at the University of Washington, is looking to graduate this spring. During her tenure at Tandon, where she has been advised by Dr. Damon McCoy, she has done research on cybercrime, natural language processing, and machine learning. She plans to move on to a career in academia where she will continue teaching and performing research in areas of computer science where ethical concerns need to be as strong as technical ones. "There is a need for a teaching curriculum that emphasizes ethics and addresses social bias. I would like to develop it.

ALUMNI PROFILE: TIM KIERAS

Classical Education Meets Contemporary Security Challenges

Cybersecurity professionals can be far from homogenous in background and training. Take Tim Kieras, a software engineer at MORSE Corp in the Boston area. Tim, who graduated in 2021 with a master's in computer science, comes from a liberal arts background. A summa cum laude graduate of Fordham University with bachelor's degrees in philosophy and classical languages, and two Master's degrees in philosophy and divinity from Fordham and Boston College, respectively, his transition from a high school teacher to a software engineer, might seem a bit surprising. But, when asked about the decision recently, he sees a clear through line from his earlier studies to his current work. "I got into philosophy because I loved the challenging and broad questions that I encountered in those classes," he observes. "While I considered academic work in philosophy, I was more drawn to finding ways to apply the skills I gained to concrete problems. After teaching for a few years, I got interested in programming and found that work with technology was a great fit for me. When I applied to the Bridge to Tandon program I didn't quite know how things would turn out, but a few years later I can say things have gone very well."

CyberByte recently touched base with Tim to ask a few more questions about his career trajectory.

CYBERBYTE: What elements do you think you brought to the field of cybersecurity from the liberal arts, and particularly from your major in philosophy?

KIERAS: While studying philosophy and classics, one thing I loved was having to be very precise with words, arguments, and ideas. I think this was great preparation for studying computer science and getting into technical work in general. More generally though, I think in cybersecurity there's a need for creative thinking that includes 'top down' or holistic perspectives to complement the detailed and technical aspects of a problem. An example is the importance of policy that is in tune with technical details without getting lost in them. To me that's where liberal arts combined with some technical skills can be a benefit.

CYBERBYTE What were the challenges in "getting up to speed" with the technical materials?

KIERAS: There were certainly challenges, but I had been introduced to programming at a fairly early age and had been teaching myself for a few years beforehand. Still though, there was plenty of background I had to catch up on during my own time. Algorithms was a tough course, but getting through it felt great. I spent plenty of time in the library, but thankfully that part wasn't a new experience for me.

CYBERBYTE: Can you briefly describe the type of work you are doing now?

KIERAS: I'm working as a software engineer at MORSE Corp, which is a defense contractor. I can't go into too many details but what drew me to MORSE was its interdisciplinary technical culture. Engineers here work on a wide variety of projects and it's been a great place for me to put my skills to work on some very tangible problems.

CYBERBYTE: You spent about a year working with Dr. Quanyan Zhu in his LARX lab at NYU Tandon. What types of projects were you involved with at the lab?

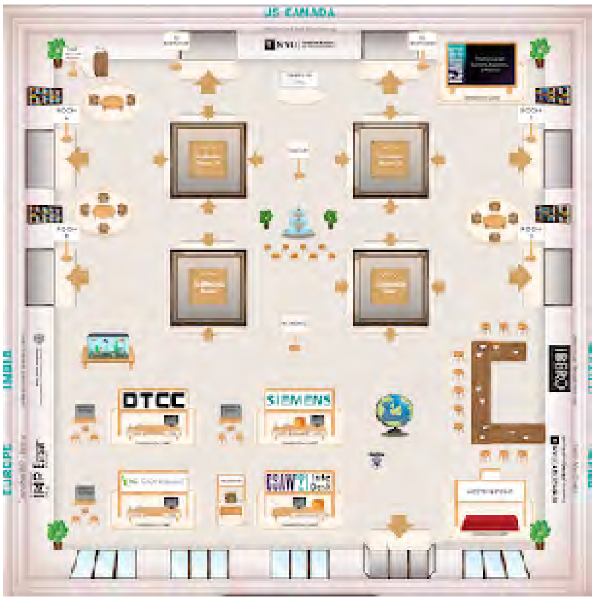
KIERAS: I worked on a project related to supply chain risk analysis and mitigation that aimed to develop a framework (called ISCRAM) for analyzing risks from potentially malicious or compromised suppliers in a large technical system. My role was mostly to provide proof-of-concept software implementing the ideas put forward by our team, but also to explore related literature, especially from cybersecurity. This was a fantastic opportunity for me to get deeper exposure to areas of engineering that my coursework in computer science wouldn't have touched on. The practical experience putting together a more complex piece of software was also extraordinarily helpful. Many thanks to Quanyan Zhu and Nasir Memon for bringing me on to the team!

CYBERBYTE: What advice might you give to someone contemplating a switch to the computer science and/or cybersecurity fields

KIERAS: Go for it, but be prepared to work hard and take the opportunities that you come across.

CSAW'21 Wrap-up: Notes from Five Days in Gather.Town

For the second year in a row, CSAW was a virtual event, with competitions, poster sessions, an industry fair, and awards ceremonies all being held online. While no online representation of CSAW can replace the excitement and camaraderie of the live version, the 2021 edition, hosted by Virtual Chair on the Gather.Town platform, did a good job of simulating its look and feel. Through the use of customizable avatars, participants were able to move through virtual meeting rooms, an auditorium, and lobby. The avatars also allowed for one-to-one interaction, so you could ask questions in a talk, or chat with a presenter in a poster session or a recruiter at the Industry Fair.



Virtual lobby from the Gather.town platform, hosted by Virtual Chair

But, while the platform was virtual, the threats described in both the challenges, and in the panel discussions and invited talks that rounded out the five day program were very real indeed. The 2021 edition of CSAW offered a snapshot of current and emerging cyber risks against a variety of attack surfaces, from integrated circuit layouts to 5G networks, particularly in a series of talks delivered on the event's opening day.

By the numbers, CSAW'21 can be summed up as follows:

- 97 universities fielded eams
- 123 teams made it to the finals in their e ent
- 323 individual competitors took part
- 22 countries were represented
- 18 exciting years of competition in the books

CSAW'21 was presented by the NYU Center for Cybersecurity, in collaboration with the NYU OSIRIS Lab, the University of Delaware's Trustworthy Computing Group, the NYU Center for Global Affair , the Interdisciplinary Centre for Cyber Security and Cyber Defense of Critical Infrastructures at IIT Kanpur, the NYU Abu Dhabi Center for Cybersecurity, Grenoble INP - Esisar and the Laboratoire de Conception et d'Intégration des Système, and Iberoamericana University, Mexico City. Corporate and government sponsors included Siemens, DTCC, iC Consult, the National Science Foundation, Facebook, Trail of Bits, Carnegie Mellon University Information Networking Institute, Security Scorecard, and Amazon Web Service. The Capture the Flag Competition was supported through challenge contributions from RET2 Systems, Vector35, DiceGang, Capsule8, Trail of Bits, Pacific Northwest National Laboratory, SecurityScorecard, perfect blue, RangeForce, Cybersecurity & Infrastructure Security Agency, CryptoHack, F-Secure, Margin Research, SimSpace Corporation, Sophos, Kroll, Microsoft Detection and Response Team, and CTF4Hire.

Note that most of the talks highlighted below can be found on the CSAW YouTube channel at https://www.youtube.com/playlist?list=PLhwo5ntex8iaamllWLLUSOUaSIV3aicV2.

Keeping the lights on and the bugs and malware out

This year's CSAW presentations illustrate the breadth of the fronts on which cyber defenses are being challenged. Dr. Martin Otto, head of the Cybersecurity Research Group for Siemens Technology, kicked things off with a keynote address that centered on the unique cybersecurity challenges of industrial infrastructures, like utilities. His presentation, entitled "Cybersecurity: Keeping the Lights On," highlighted how longer system equipment lifecycles and the need for continuous availability call for different approaches than that of conventional computer systems, as well as how much graver the consequences of a hack can be. As he phrased it in his presentation, "If you mess up in IT Security, you don't get access to Facebook for a day," whereas an attack on utilities could mean, "the whole East Coast goes dark." His talk recommended ways the industry can build and operate more secure systems, and included an appeal for more research—both academic and industrial—to protect this key industrial sector.

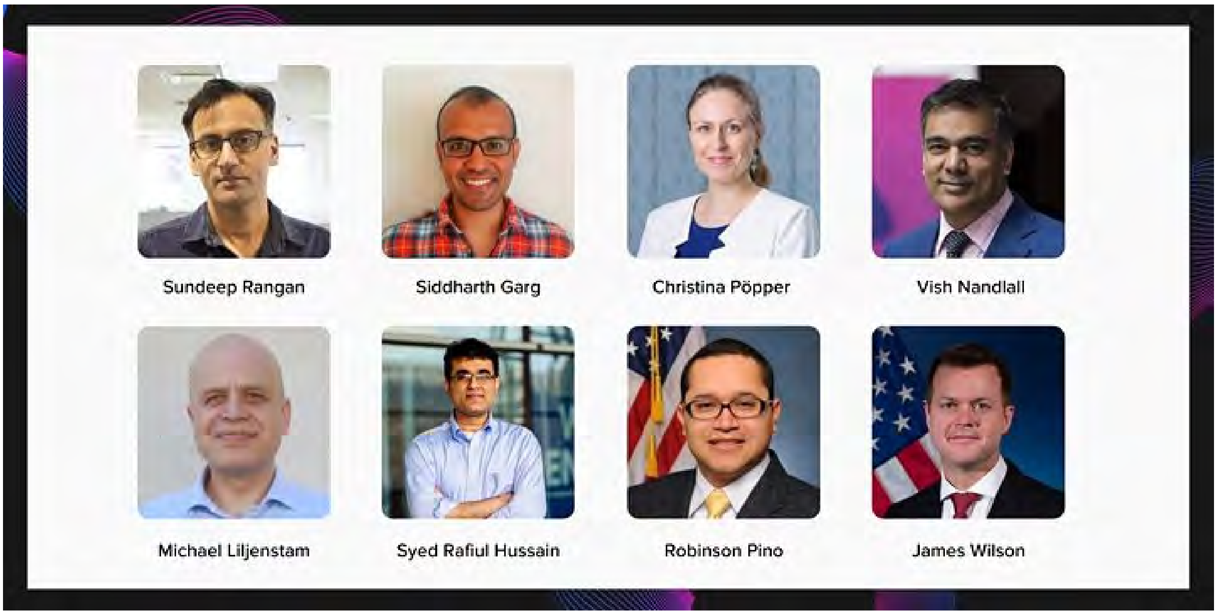
Following the keynote, Dr. Johann Knechtel, a research scientist with the Design for Excellence Lab at NYU Abu Dhabi, shared insights on an emerging supply chain security issue: vulnerabilities in the design and production of integrated circuits. In particular, he addressed how proactively hardening the IC design can hinder adversarial activities that may occur later on in the supply chain. Pointing to the lack of a "holistic approach" to current security in IC development and production, he noted that "layout-level security closure works better if integrated with 'secure by design' CAD flows." Knechtel closed his presentation by announcing a new competition on this topic to be held at the International Conference on Physical Design in March 2022.

Dr. Hammond Pearce of the NYU Center for Cybersecurity closed out this trio of presentations by sharing insights from a study on bugs and design flaws in the popular GitHub Copilot programming assistant. With his Tandon CCS colleagues Baleegh Ahmad (Ph.D. student), Dr. Benjamin Tan (now an assistant professor at the University of Calgary), Dr. Brendan Dolan-Gavitt, assistant professor of computer science and engineering, and Dr. Ramesh Karri, Hammond created and tested 1,692 programs in Copilot, and found that about 40 percent of the programs included bugs or design flaws that could be exploited by an attacker. A takeaway of the study was that Copilot should be paired with appropriate security-aware tooling during both training and generation to minimize the risk of introducing security vulnerabilities. You can read the paper that documents Hammond's study results at https://arxiv.org/abs/2108.09293.

Upping the ante:

How 5G networks are preparing for next-generation attacks

To say 5G networks and applications are rapidly multiplying is a serious understatement. One survey estimates that the global market for 5G infrastructure will grow by about 800% in the next five years, from $12.9 billion in 2021 to $115.4 billion in 2026 (https://www.businesswire.com/news/home/20210910005400/en/Global-5G-Infrastructure-Market-Report-2021-Market-Is-Expected-to-Grow-From-12.9-Billion-in-2021-to-115.4-Billion-by-2026---ResearchAndMarkets.com).



With so much being invested in this technology, defensive strategies for networks and applications must always be one step ahead of the malicious actors who will inevitably try to exploit them. Recognizing how large the stakes have grown, NYU WIRELESS at NYU Tandon hosted a panel to discuss the threats that are multiplying as quickly as the technologies themselves. These include massive scale denial of service (DoS) attacks, man-in-the-middle (MitM) attacks, hardware and software Trojans, resource misuse, data breaches, and attacks launched from within the network or edge cloud itself.

Hosted by Dr. Siddharth Garg, a faculty member for both the NYU Center for Cybersecurity and NYU WIRELESS, and Dr. Sundeep Rangan, associate director of NYU WIRELESS, the panelists, selected to represent industry, academia, and government sectors, were:

- Michael Liljenstam, principal researcher at Ericsson Research
- Vishwamitra Nandlall, vice president of tech strategy and ecosystems at Dell Technologies
- Syed Rafiul Hussain, assistant professor of computer science and engineering, The Pennsylvania State University
- Christina Pöpper, assistant professor of computer science and principal investigator for the Cyber Security and Privacy Lab at NYU Abu Dhabi
- Robinson Pino, program manager at the U.S. Department of Energy
- James Wilson, program manager of the Microsystems Technology Office, Defense Advanced Research Projects Agency

Topics ranged from the impact of disaggregation of network functions, which "creates more points of interaction that equals greater risk," to how protecting privacy will require "trade-offs" in utility, and the need for "zero trust supply chains" in which trust is not taken as a given, despite the general assumption that the network is a trusted party. In addition, the discussion touched on the expanding positive and negative potentials of artificial i telligence and machine learning.

Perhaps the comment that best summed up the importance of securing these technologies came from Nandlall of Dell Technologies who observed that "5G is the tipping point where cellular becomes critical infrastructure." In light of this change, industry, academia and government agencies need to heed the words of Penn State's Hussain and recognize that "security and privacy must be first class citizens" when it comes to setting priorities.

Temple-Raston Honored with Cyber Journalism Award

Closing out the opening day activities was the presentation of the CSAW'21 Cyber Journalism Award to Dina Temple-Raston, a senior correspondent for The Record, a cyber and intelligence news service. Temple-Raston who covered issues in counter-terrorism and technology for National Public Radio for 15 years, received the award for her audio and print feature for NPR entitled "A 'Worst Nightmare' Cyberattack: The Untold Story of the SolarWinds Hack."

In an informal conversation celebrating her award, Temple-Raston virtually sat down with Dr. Ramesh Karri to answer a few questions about the article, starting with why she chose to do a "deep dive" on this topic. She replied that, "it was really hard for anyone to get their arms around what the hack really was." Through stories like hers, she believes people can now better articulate the what, when, why, and how of the attack. "That's what I think is really important about cyber journalism, and why, in fact, I left NPR to go to The Record...to explain these topics in a way that someone's mother could understand."

For those wondering how Russia became such a hacker haven, she described what she called "a devil's pact" between Russian hackers and their government, which boils down to "don't hack us and we'll look the other way." That is, the actions are not explicitly sanctioned by the government, but the government is doing nothing to stop them either. Noting that the Chinese government now has "started to steal plays out of this particular playbook," she stressed that it is more important than ever that "there be some sort of agreement between allies, enemies, frenemies to say, 'OK, this is a set of cyber norms where we just don't hack this kind of thing.' And that hasn't happened. This may now be our best chance to get there because people are watching in a way they hadn't been before."

It may also be the right time to finally implement the common sense strategies the industry has long talked about but never employed. "The (Biden) executive order that came out not too long after SolarWinds started to address a lot of these things that basically are 'cyber hygiene'." Though she notes that this phrase has become "a buzzword nobody really listens to," with SolarWinds heightening an awareness of the consequences, perhaps basic, common sense strategies will finally become the norm.

You can read/listen to Temple-Raston's award winning article at (https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack).

Honoring the Best of CSAW'21

One benefit of being a virtual conference is that we were able to hear the winners of CSAW competitions all over the world announced in real time. In that spirit, we decided to share the names of all the first place winners here, no matter where they competed. A complete list of all award winners can be found on the CSAW website at https://www.csaw.io/2021winners.

Badges and certificates awarded to CSAW '21 competition winners.

APPLIED RESEARCH COMPETITION, 1ST PLACE WINNERS

- Europe | Sinem Sav (EPFL Switzerland), presenting POSEIDON: Privacy-Preserving Federated Neural Network Learning
- MENA | Ofek Kirzner (Tel Aviv University, Israel), presenting An Analysis of Speculative Type Confusion Vulnerabilities in the Wild
- US-Canada | Erin Avllazaga (University of Maryland, College Park), presenting When Malware Changed Its Mind: An Empirical Study of Variable Program Behaviors in the Real World

CAPTURE THE FLAG 1ST PLACE WINNERS

- Global and US-Canada PPP, Carnegie Mellon University (USA)
  Albert Gao, Anish Singhani, Parth Shastri, Robert Chen

- Europe | Tower of Hanoi, Italy
  Daniele Mammone, Politecnico di Milano; Bruno Halltari, Università degli Studi di Milano; Marco Meinardi, Politecnico di Milano; Tommaso Fontana, Università degli Studi di Milano

- India | InfoSecIITR, IIT Roorkee
  Aryaman Behera, Kartikey Kumar, Mohit Sharma, Shubhang Tripathi

- MENA | Fword, INSAT, Tunisia
  Mohamed Arfaoui, Oussema Majbri, Semah BenAli

- Mexico | Mayas, Mexico
  Luis Adrian De la Rosa, Universidad Autonoma de Nuevo Leon; Alejandro Jacobo, Universidad Autonoma de Nuevo Leon; Ivan Medina, Universidad Autonoma de Coahuila; Bryan Enrique González Vélez, Escuela Superior de Cómputo del Instituto Politécnico Nacional

CYBER SECURITY CHALLENGE FOR HIGH SCHOOL (MEXICO) 1ST PLACE WINNERS

- ● ASFC Dream Team, Colegio American School Foundation of Chiapas A.C.
  Ximena Cardenas Topete, Carla Tovilla Marin, Jesus Emiliano Pastrana Lopez

  Profesor: Abel Castellanos Espinosa

EMBEDDED SECURITY CHALLENGE 1ST PLACE WINNERS

- Europe Research | TRX Research Labs, Sapienza Universita di Roma, Italy
  Pietro Borrello, Dario Petrillo, Daniele Tarantino, Noemi Palmeri

  Advisor: Leonardo Querzoni

- Europe Technical | TRX Technical Labs, Sapienza Universita di Roma, Italy
  Qian Matteo Chen, Matteo Almanza, Pasquale Caporaso, Cristian Assaianate

  Advisor: Leonardo Querzoni

- India Research | ZeroLeakers, IIT Madras
  Prithwish Basu Roy, Pallavi Borkar, Sandip Saha, Girinath P

  Advisor: Chester Rebeiro

- India Technical | SDSLabs, IIT Roorkee
  Manas Chaudhary, Gaurav Genani, Priyansh Rathi, Mayank Mittal

  Advisor: Debiprasanna Sahoo

- US-Canada + MENA Technical | Rackets, Georgia Institute of Technology
  Spencer Hua, Ammar Ratnani, Zelda Lipschutz, Suhani Madarapu

  Advisor: Allen Stewart

- US-Canada + MENA Research | SENTRY, King Abdullah University of Science and Technology
  Ioannis Zografopoulos, Panagiotis Karamichailidis

  Advisor: Charalambos Konstantinou

HACK3D 1ST PLACE WINNERS

- Family.py, NYU Abu Dhabi
  Abdul Gomda, Dev Kalavadiya, Hassan Hamdani, Soumen Mohanty

LOGIC LOCKING CONQUEST 1ST PLACE WINNERS

- Texas Magicians, Texas A&M University
  Zhaokun Han, Mustafa Munawar Shihab

  Advisors: Shayan Omais Mohammed, Yiorgos Makris, Jeyavijayan Rajendran

POLICY COMPETITION 1ST PLACE WINNERS

- Team 9 - Ransomware: Payment Policies, Cambridge University, United Kingdom
  Adam Ó Conghaile, Bence Borbely, Jerry Li

CCS EVENTS

NYU TANDON SCHOOL OF ENGINEERING

UNIVERSITY OF DELAWARE

IEEE WORKSHOP (VIRTUAL)

Reliable and Resilient Digital Manufacturing

https://r2dm-workshop.github.io/

SEPTEMBER 16 & 17
10:00 AM - 3:00 PM EDT

Register at : https://r2dm2021.eventbrite.com/

NSF

IEEE

CCS Faculty Organize IEEE Workshop on Reliable and Resilient Digital Manufacturing

A team of faculty members with ties to the NYU Center for Cybersecurity joined forces this fall to organize an online workshop on the topic of Reliable and Resilient Digital Manufacturing (R2DM) for the Institute of Electrical and Electronics Engineers (IEEE). Held September 16-17, 2021, the workshop was organized by Professors Nikhil Gupta and Ramesh Karri; Dr. Hammond Pearce, and an NYU alumnus, Professor Nektarios Tsoutsos from the University of Delaware. It featured presentations by nine invited speakers on topics ranging from security, privacy, and innovations in design, to human-in-the-loop assembly and embedded systems. In addition, Dr. Andrew Wells from the National Science Foundation and Paul Huang from the Office of Naval Research delivered keynote addresses.

On the second day of the workshop five students conducting research work in digital manufacturing presented talks, which were judged by Professor Mihalis Maniatakos of the Electrical and Computer Engineering Department at NYU Abu Dhabi, and Yan Lu from the National Institute of Standards and Technology. Students from the University of Delaware took top honors, with the first place award going to Dimitris Mouris, and Lars Folkerts receiving second place honors. Harsh Srivastava from the National Institute of Technology Warangal took third place.

Sponsored by the National Science Foundation, the workshop drew 184 registrants. A second workshop on the topic of digital manufacturing is currently being planned for early Summer 2022.

Awards and Honors

Dr. Brendan Dolan-Gavitt, an assistant professor in the Department of Computer Science and Engineering and a faculty member with NYU's Center for Cybersecurity, was named a recipient of a 2022 Faculty Early Career Development Award from the National Science Foundation. Known as a CAREER Award, it is given to "early-career faculty who have the potential to serve as academic role models in research and education." Dolan-Gavitt received the award for his achievements in improving software vulnerability testing and education.

The honor comes with a fi e-year, $500,000 research grant. Dolan-Gavitt will use these funds to continue his work in applying artificial intelligence to the creation of synthetic vulnerabilities. Specificall , the project employs large language models, trained on code to synthesize vulnerabilities that are both realistic and diverse. In addition, the project will enable placement of vulnerabilities in hard-to-discover paths, allow new vulnerability classes to be added quickly with a customized domain-specific language, and automatically generate exploits for each vulnerability.

This avenue of research is equally important to academia, as it provides real-world data and scenarios for use in classroom projects and cyber competitions. As an advisor to Tandon's annual CSAW event since joining the faculty in 2015, Dolan-Gavitt has witnessed firs -hand the educational value of its "Capture the Flag" competition. "These types of competitions are extremely popular and effective means of teaching a variety of cybersecurity skills, but they require large amounts of time, money, and expertise to create and manage," he explains. "If the creation of the challenges can be partially or wholly automated, it could bring new educational opportunities within reach of a broader and more diverse population of students by dramatically lowering costs and reducing the time and effort needed."

In receiving the 2022 award, Dolan-Gavitt joins seven of his CCS colleagues who have previously won this recognition. It also continues NYU Tandon's strong track record in this arena, as more than half of the junior engineering faculty members at NYU Tandon have received CAREER Awards or similar young-investigator honors, including 10 since 2019.

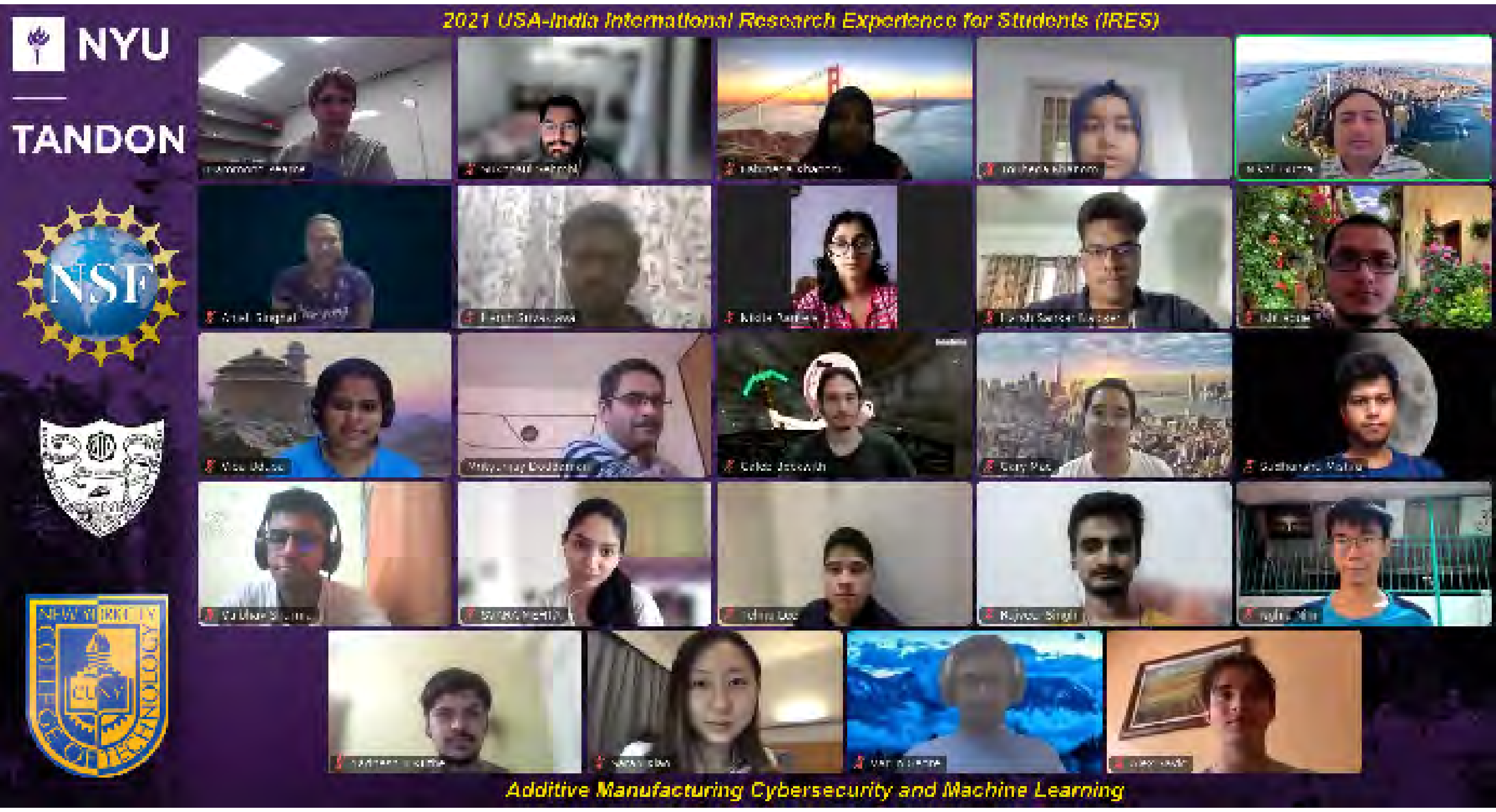
Danny Yuxing Huang (1st Photo at left), an assistant professor with affiliations in both the Center for Cybersecurity and the Center for Urban Science and Progress at NYU, has been named by Consumer Reports as one of three Digital Lab Fellows for 2021-2022. Supported by the Alfred P. Sloan Foundation, the Digital Lab Fellows program supports research to uncover and address emerging consumer harms. As a Digital Lab fellow, Huang will co-create a strategy to "improve the usability of IoT Inspector, scale up the user-contributor community, and attract more users and researchers toward this open data science." The wider benefit of this research will be a broader understanding of security and privacy issues as they apply to smart home IoT devices.

Congratulations to the NYU Cyber Fellows who have won recognition at two different cyber defense competitions. First, a team consisting of Quoc Duong, Diana Xu, Sonia Rahman, Clayton Barbier, and Brandon Sloane competed in the U.S.Department of Energy (DOE) CyberForce® Program Competition and earned a place in the top 10. A total of 120 college and university teams from 33 states took part in the two-week competition this November that challenged participants to harden and secure systems of a hydropower company—along with the systems of one of its recently acquired subsidiaries—against a malicious cyberattack, all while maintaining service for customers.

A month earlier at the Cybertech NYC conference, NYU Cyber Fellow Zvi Greenspan (pictured in photo left) and his teammate Abraham David Minkowitz, took first place in the Cybertech Student Cup, hosted by Cyberbit (https://www.linkedin.com/company/cyberbit/).

CCS News Round-up

Manufacturing Security Initiative Pairs U.S. and Indian Students for Summer Research Experience


2021 USA-India International Research Experience for Students (IRES)
NYU
TANDON
NSF
NEW YORK CITY COLLEGE OF TECHNOLOGY
CUNY
Additive Manufacturing Cybersecurity and Machine Learning

In the summer of 2020, the National Science Foundation (NSF) International Research Experience for Students (IRES) program awarded a three year grant to faculty at NYU Tandon and the NY City College of Technology in the U.S., and the National Institute of Technology – Karnataka (NITK) in India to develop a summer research program focused on 3-D manufacturing. Organized by Professors Nikhil Gupta and Ramesh Karri at NYU, in collaboration with Professor Mrityunjay Doddamani of NITK, the program paired 9 US-based undergraduate students with 11 undergraduate students from top engineering institutions across India to work on research projects related to security and other issues in 3D manufacturing.

As originally planned, the program would have been held at NITK, giving the US students a chance to not only experience real world research in a major science and technology research hub, but also have opportunities for cultural interactions. Though Covid 19 restrictions kept everyone in a virtual environment, the students were able to share unique details and local knowledge from their hometowns, states, and countries, including comparing local foods and recipes, and playing games together.

Under the supervision of Dr. Hammond Pearce and Gary Mac, the students worked collaboratively on a variety of projects, including using statistical modeling and machine learning to detect defects maliciously inserted into 3D-printable CAD file , and computer vision algorithms to gauge properties of 3D-printed composites and metals. Participants also helped to organize the debut of the Hack3D Summer challenge by creating mini-challenges and promoting the competition to other universities.

Applications for the 2022 program will be available later this year.