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 benefi .

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.

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 fi e day program were very real indeed. The 2021

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

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.

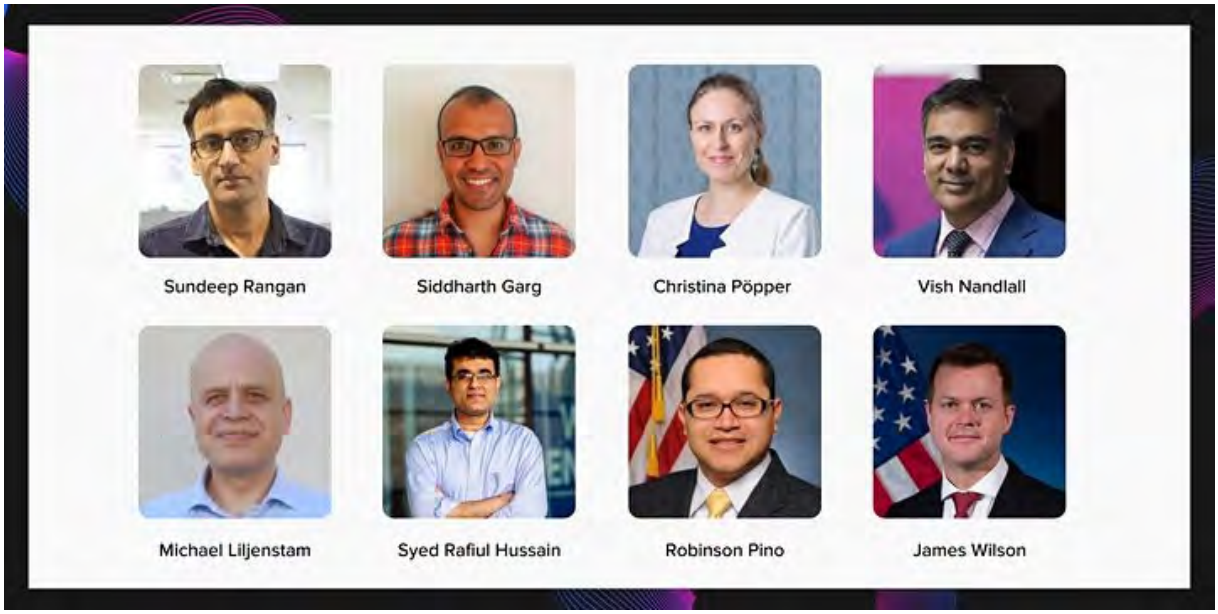
Following the keynote, Dr. Johann Knechtel, a research scientist with the Design for Excellence Lab at NYU Abu Dhabi, shared insights on an emerging supply chain security issue: vulnerabilities in the design and production of integrated circuits. In particular, he addressed how proactively hardening 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 certific tes 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

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 fi e 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.