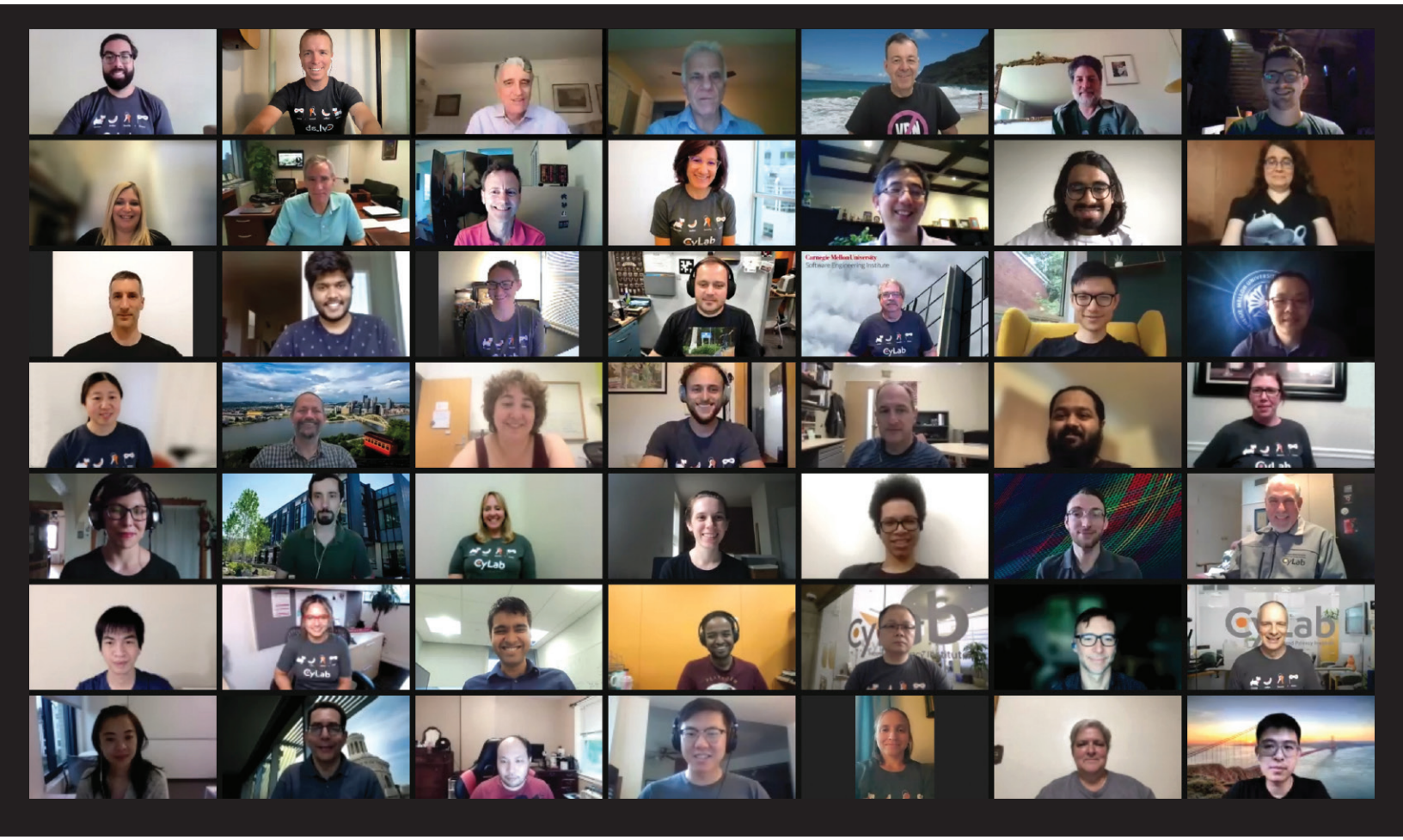
2020–2021 CYLAB **YEAR IN REVIEW**



CyLab Carnegie Mellon University
Security and Privacy Institute

LETTER FROM THE **DIRECTOR**

DEAR FRIENDS

As I write this letter in July 2021, CyLab is starting to open up again. I've removed the layer of dust that settled on my office while I was working from home and recycled stacks of papers and mail that sat on my desk at work untouched for the past 16 months (obviously I didn't need them). We've all made adjustments in our lives to accommodate the new normal and now we're starting to face yet another new normal that looks a little different than the old normal. Many of us have become really good at productive remote work and for some working from home means a big reduction in commute time and easier childcare arrangements. Nonetheless, a lot of what we do in CyLab really benefits from in-person interactions. I'm excited to resume face-to-face meetings with collaborative research groups and chance meetings in the CyLab kitchen.

The pandemic year was tough on mental and physical health, and just getting through the pandemic year more or less in one piece was an accomplishment for many. I had goals for CyLab for the year that I quickly tossed aside as my calendar filled up with endless Zoom planning meetings. But despite the challenges, I believe that we in CyLab did more than just survive; in many ways we thrived.

As you will read in this issue, we launched CyLab Africa, collaborated with our friends down the street at the University of Pittsburgh on a new center to combat extremist hate, expanded our privacy engineering educational offerings, designed and evaluated a privacy icon for the State of California, developed the fastest ever open-source intrusion detection system, conducted first-of-their-kind analyses of cryptocurrency derivatives markets, and much, much, more.

Throughout the year, CyLab people were busy conducting new research and presenting their results at virtual events. We held our annual partners conference online in 2020 and are preparing to do it again in 2021. We also co-hosted the 2021 Conference on Privacy Engineering Practice and Respect (PEPR), the largest ever gathering of privacy engineers with over 500 participants.

And, of course, we taught our classes and advised our students. We acquired microphones and ring lights for our home offices, swapped Zoom teaching advice, learned the ins and outs of giving exams online, and figured out how to hold educational class discussions in breakout rooms. We watched students tune into our classes from their beds, and sometimes lean back and fall asleep.

On a personal level, I've heard from colleagues who adopted new pets, improved their diets, planted vegetable gardens, renovated their kitchens, and started regular exercise routines. I personally played a lot of pickup soccer and began playing the bass flute. I also started writing a privacy column for Communications of the ACM and am now co-hosting the "Over the Rainbow" podcast for IEEE Security and Privacy Magazine.

The 2020-21 academic year was certainly one for the books, and I'm proud of the way the CyLab community managed to survive and flourish during challenging times. I'm looking forward to figuring out the new, new normal with my colleagues and friends.

Lorrie Cranor

Director and Bosch Distinguished Professor in Security and Privacy Technologies, CyLab

FORE Systems Professor of Computer Science and of Engineering & Public Policy

CONTENTS

CYLAB RESEARCH
IMPACTS NEW PRIVACY LAW

In March, a groundbreaking privacy law in California was updated thanks to the hard work and expertise of CyLab researchers.

Additional regulations added to the California Consumer Privacy Act (CCPA) to include adoption of a Privacy Options icon came just as the team of researchers that helped lawmakers design the blue button were getting ready to share results of their research process that informed the icon design.

A California privacy law will utilize a privacy icon designed by researchers in Carnegie Mellon University CyLab and the University of Michigan's School of Information.

Researchers from Carnegie Mellon University CyLab and the University of Michigan presented a paper at CHI 2021, the ACM Conference on Human Factors in Computing Systems—considered the premier peer-reviewed publication venue for Human-Computer Interaction research—on their work to help consumers opt out of having their private information sold by merchants, social media companies and other businesses.

The California act was ratified in 2018 and went into effect in 2020, but several additional regulations were announced March 15. The CCPA is a comprehensive privacy law that shares some similarity with Europe's General Data Protection Regulation. Among other things, it says companies and organizations that profit from personal information must provide a dedicated link on their websites that allows consumers to tell companies "do not sell my personal information."

The law allows a button to accompany the link for this opt-out purpose, so it became the job of the Office of the Attorney General (OAG) in California to figure out what that could look like.

"It is well known that privacy policies are lengthy and full of jargon," said CyLab's Hana Habib, a Ph.D. candidate at the Institute for Software Research (ISR) at Carnegie Mellon. "Privacy choices are also hard to find on a website. Simple icons with the right labeling can communicate concepts quickly and concisely across languages and cultures, but it is important to get it right through user testing."

Since depicting the concept of privacy seemed difficult, the team developed 11 icons they thought best represented the concepts of choice, opting out and not selling personal information. They added an icon created by the Digital Advertising Alliance industry group and tested all 12 with participants recruited from Amazon's Mechanical Turk.

Initial results suggested text was needed to make sense of the icon, so in a second study they came up with and evaluated 16 phrases, including "Do Not Sell My Personal Information," which is the text required by the CCPA, and potential alternatives such as "Privacy Choices" and "Don't Sell."

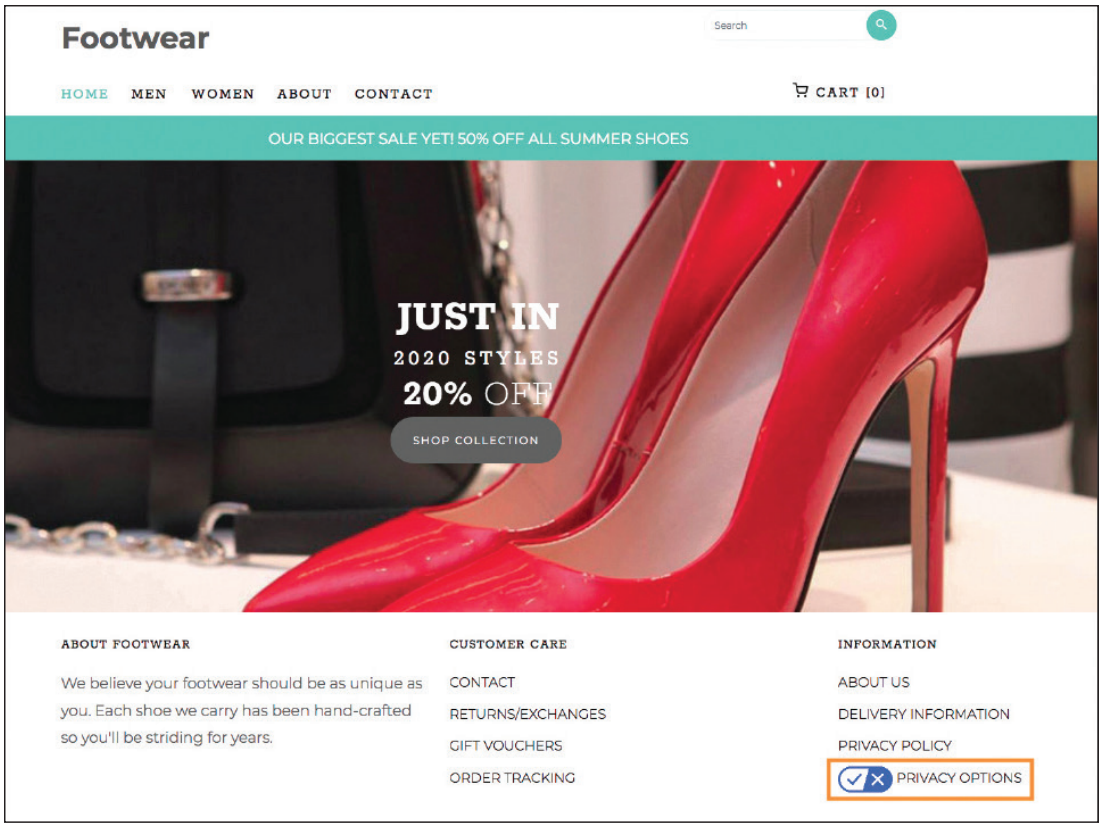
Five leading text choices were combined with three top icon picks and tested on a fictitious shoe website. In this study, a blue stylized toggle icon emerged as the preferred design to convey choices. Together with the link text "Privacy Options" this icon was highly effective at conveying to people the presence of privacy choices.

"We hope that policymakers and researchers collaborating in this way can become a model approach towards more usable consumer notices and controls in privacy and other contexts."

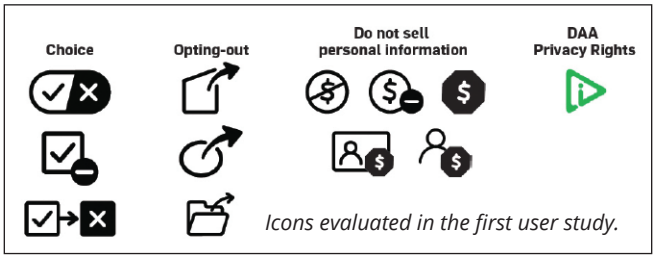
Lorrie Cranor, *Director and Bosch Distinguished Professor in Security and Privacy Technologies, CyLab*

FORE Systems Professor of Computer Science and of Engineering & Public Policy

---



In the combination icon and link text study participants were shown this screenshot of a fictitious footwear website with an icon and link text highlighted.



Icons evaluated in the first user study.

The Office of the Attorney General initially picked an icon of its own design. After the CyLab team tested it and found that it caused too many misconceptions, the OAG reconsidered and eventually selected the team's recommended icon.

"This work in collaboration with the OAG demonstrates the importance of involving user testing in policymaking processes to ensure that resulting controls for consumers are actually useful and usable," said senior author Florian Schaub, assistant professor at the U-M School of Information. "I really commend the Office of the Attorney General for working with us and ultimately following our research-based recommendations."

The bottom line of their various user tests:

- Icons for privacy choices should be rooted in simple and familiar concepts rather than attempting to visualize abstract privacy concepts or data practices.
- Icons should be accompanied by link texts, at least initially, to aid comprehension and allow consumers to become familiar with them.
- Another icon, the DAA AdChoices icon, is still not familiar and frequently misunderstood by people, even though it has been around for years.

At this point the Privacy Options icon is optional. It is up to companies whether they adopt it or not.

"We hope that companies and also policymakers in other U.S. states and at the federal level will decide to adopt it, and thus give consumers an easily recognizable entry point to a company's privacy settings," said Yixin Zou, doctoral candidate at the U-M School of Information.

The researchers say their work demonstrates the importance of including user research and usability testing in policy and rulemaking processes, especially when laws and regulations require providing notices or controls to consumers. Otherwise, they say, there's a risk that intended consumer protections don't materialize in practice or even mislead consumers, as has been the case with lengthy and vague privacy policies or difficult to find privacy settings and opt-outs.

"We hope that policymakers and researchers collaborating in this way can become a model approach towards more usable consumer notices and controls in privacy and other contexts," said Lorrie Faith Cranor, director of CyLab and a professor in the departments of Engineering and Public Policy and the ISR.

THE WORLD'S FASTEST **OPEN-SOURCE INTRUSION DETECTION SYSTEM IS HERE**

The system achieves speeds of 100 gigabits per second using a single server.

Intrusion detection systems are the invisible intelligence agencies in computer networks. They scan every packet of data that is passed through the network, looking for signs of any one of the tens of thousands of different types of cyberattacks they're aware of.

As Internet speeds continue to increase, so too does the amount of data that passes through. To keep up, intrusion detection systems have grown into giant racks and stacks of servers, driving energy costs up for organizations that rely on them for protection.

> **"What was previously possible with 100-700 processor cores and a whole rack of machines, we can now do with five processor cores in a single server. We created one pizza box-sized machine to do the work of a whole room of servers."**
>
> ***Justine Sherry,*** *Assistant Professor, Computer Science Department, School of Computer Science*

That's all about to change. Researchers in Carnegie Mellon University's CyLab have developed the fastest-ever open-source intrusion detection system—one that achieves speeds of 100 gigabits per second using a single server.

"What was previously possible with 100-700 processor cores and a whole rack of machines, we can now do with five processor cores in a single server," says CyLab's Justine Sherry, an assistant professor in the Computer Science Department (CSD) in the School of Computer Science.

The researchers presented their work at the USENIX Symposium on Operating Systems Design and Implementation in November.

The system achieves speeds of 100 gigabits per second using a single server.

Key to the researchers' success is the use of a field-programmable gate array (FPGA), an integrated circuit for which users can write code and customize, hence "field-programmable." The researchers programmed the FPGA to be tailored for the sole job of intrusion detection and wrote algorithms which can't run on traditional processors and are significantly faster.

When placed in a network, Sherry says that an average of 95 percent of data packets are processed by the FPGA on its own, while the other five percent are passed on to central processing units when it becomes overwhelmed, hence the necessity of five processor cores in their system.

"The FPGA does most of the work, but some of it still goes to the processors," Sherry says.

The result in energy-savings is enormous: their intrusion detection system uses 38 times less power using an FPGA than hundreds of processing cores would in performing the same work.

"It's like your electricity bill used to be $100, and now it's $3," says Sherry. "We created one pizza box-sized machine to do the work of a whole room of servers."

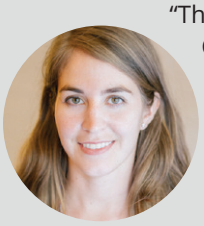
The researchers' code is open-sourced and available for download on GitHub.

CMU-AFRICA AND CYLAB AIM TO **IMPROVE FINANCIAL INCLUSION IN EMERGING ECONOMIES**

Despite COVID-19's effects on economies around the globe, there is a huge amount of projected growth in the African economy over the next five years. On top of that, the pandemic itself has driven more and more people to transact money digitally, making financial technologies ever more important.

But in order to drive financial inclusion alongside that growth, experts say big improvements need to be made to the security and resilience of the continent's financial technologies and infrastructure.

That's why CyLab and CMU-Africa launched the CyLab-Africa initiative, which aims to improve the cybersecurity of financial systems in Africa and other emerging economies.



"The projected growth in Africa is fragile," says CyLab's Giulia Fanti, an assistant professor of electrical and computer engineering and a principal investigator (PI) on the grant. "It depends on improving access to financial technologies, as well as building public trust in those technologies. Cybersecurity is a critical requirement for both."

Major cyberattacks have plagued the African economy in the past several years. Last October, a mobile money fraud hack cost Ugandan banks $3.2 million in stolen funds. The year before, security firm Symantec revealed that malicious hackers had been targeting west African banks since mid-2017.

"These major hacks have slowly eroded trust in our financial systems," says Assane Gueye, an assistant teaching professor at CMU-Africa and a PI on the project. "When you compare Africa to other continents, the cybersecurity infrastructure just isn't there."

Underneath these hacks is a myriad of issues in cybersecurity capacity. As of May 2020, only 12 countries of the 55 African Union members had a national cyber strategy and only 13 had a national computer emergency response team. While Africa isn't the only place on the planet with cybersecurity issues, its cybersecurity capacity is lagging across multiple dimensions, according to the Global Cybersecurity index.

> **"CyLab-Africa aims to address the unique and fragile environment in Africa right now and enable financial inclusion through access, trust, and resilience."**
>
> ***Vijayakumar Bhagavatula,*** *Director of CMU-Africa, U.A. & Helen Whitaker Professor of Electrical and Computer Engineering*

"CyLab-Africa aims to address the unique and fragile environment in Africa right now and enable financial inclusion through access, trust, and resilience," says Vijayakumar Bhagavatula, the director of CMU-Africa and a professor of electrical and computer engineering.

The team's plan for improving financial inclusion involves four initial research thrusts:

1. Assessing the cybersecurity risk to African financial inclusion
2. Developing tools for securing financial infrastructure
3. Developing tools for threat intelligence sharing and diagnosis
4. Designing training programs for cybersecurity workforce development

Continued on page 8

"The initiative will not only capitalize on CMU-Africa as a recognized research and education leader in sub-Saharan Africa, it will also leverage the exceptional research and education capabilities here in CyLab and CMU's Software Engineering Institute," says CyLab director Lorrie Cranor, a professor in the Department of Engineering and Public Policy and the Institute for Software Research.

While CyLab-Africa will initially focus on the financial sector, the ultimate goal is to advance security and privacy research and education in emerging economies more broadly.

Currently, seven faculty at Carnegie Mellon's Pittsburgh, Pennsylvania and Kigali, Rwanda campuses are involved in CyLab-Africa.

- Vijayakumar Bhagavatula, Director of CMU-Africa; U.A. & Helen Whitaker Professor of Electrical and Computer Engineering
- Lorrie Cranor, Director of Carnegie Mellon University CyLab and Bosch Distinguished Professor in Security and Privacy Technologies; FORE Systems Professor in Engineering and Public Policy and the Institute for Software Research

CMU AND PITT LAUNCH CENTER DEDICATED TO **COMBATING EXTREMIST HATE**

Carnegie Mellon University and the University of Pittsburgh have jointly launched a new center to study extremist hate.

Scholars at both universities are partnering through the Collaboratory Against Hate — Research and Action Center to develop effective tools that inhibit hate's creation, growth, and destructive consequences.

The center brings together the collective expertise from all relevant disciplines—including computer science, data science, social sciences, psychology, psychiatry, and the law—as collaborators seek to better understand and combat hatred based on race, ethnicity, religion, gender identity, sexual orientation, and other prejudices.

The collaboratory is being led by two top experts in extremist hate groups and cybersecurity: Distinguished Professor of Sociology and Bettye J. and Ralph E. Bailey Dean of Pitt's Kenneth P. Dietrich School of Arts and Sciences, Kathleen Blee, and Lorrie Cranor, director and Bosch Distinguished Professor in Security and Privacy Technologies in CMU's CyLab. The universities are in the process of building out the center's research team and welcome engagement from experts at each institution, as well as from community groups.

"The spread of extremist hate is undeniably insidious and increasingly dangerous. We have witnessed its violent consequences in our own community, including the horrific attack at the Tree of Life synagogue building, and have also seen this epidemic pose an existential threat to our nation's democracy," said Carnegie Mellon President Farnam Jahanian. "CMU and Pitt have a unique opportunity to work against this socially destructive force and enhance our multipronged efforts against all forms of hatred."

"The University of Pittsburgh is excited to grow our close collaboration with CMU," said Pitt Chancellor Patrick Gallagher. "We've launched Collaboratory Against Hate with a clear purpose: to mobilize our experts and assets together so that we can better understand and address extreme hate—in its many iterations and implications—across the world."

> **"The spread of extremist hate is undeniably insidious and increasingly dangerous."**
>
> ***Farnam Jahanian,*** *President, Carnegie Mellon University*

The center aims to develop effective interventions to inhibit every stage in the creation and growth of extremist hate, as well as interventions to minimize its impacts. Researchers will study how extremism originates and circulates, how it shapes extremist views and fosters polarization in society, and how it provokes harmful and illegal acts, with a focus on its effects on minoritized and marginalized groups in society.

- Giulia Fanti, Faculty PI for CyLab-Africa; Assistant Professor in Electrical and Computer Engineering
- Assane Gueye, Faculty PI for CyLab-Africa; Assistant Teaching Professor at CMU-Africa

- Edwin Kairu (shown left), Faculty PI for CyLab-Africa; Instructor at CMU-Africa
- Vyas Sekar, Faculty PI for CyLab-Africa; Tan Family Associate Professor in Electrical and Computer Engineering
- Conrad Tucker, Faculty PI for CyLab-Africa; Arthur Hamerschlag Career Development Professor in Mechanical Engineering

The CyLab-Africa initiative is supported by a grant from the Bill & Melinda Gates Foundation.

The center is partnering with various stakeholders—ranging from victimized communities and advocacy groups to technology companies and policymakers—to better understand underlying issues and design intervention tools. These tools will aim to address different levels of radicalization and can be used by people, groups, and institutions with varying needs and agendas.

"This is fundamentally an interdisciplinary problem," Cranor said. "As our machine learning experts create new ways to detect hate speech and misinformation, it's important that they partner with social scientists who are researching the thought processes of extremist groups. Together, we can make greater progress toward understanding how these groups communicate, recruit and organize, and, hopefully, create interventions that will help reduce the spread of hate."

Blee, who has studied white supremacism for more than 30 years, said that extremist hate groups have radically changed the way they operate and mobilize people to advance their agendas. The internet and social media not only provide groups with a vast arena for recruitment, but also places where they can hide.

"They've made the distribution, mobilization and spread of online hate much harder to monitor and prosecute. It's also more difficult to decipher the extent to which virtual communities of hate are simply reinforcing each other or being pushed by organized extremist organizations," Blee said. "That's created challenges for researchers and law enforcement who are trying to understand how these groups work and how to intervene."

The idea for this center came from the long-standing partnership between Carnegie Mellon's President Emeritus Jared Cohon and Pitt's Chancellor Emeritus Mark Nordenberg. While serving together on a committee created by the Jewish Federation of Greater Pittsburgh in the immediate aftermath of the attack at the Tree of Life synagogue, they were asked to explore ways in which the community might constructively respond to the hate-fueled violence that occurred that day. Cohon and Nordenberg then worked with a group of faculty members at both universities, who contributed to the establishment of the center.

"I'm enthusiastic because, as with so many other partnerships throughout our history, CMU and Pitt complement each other very well," said Cohon, who is also a CMU University Professor. "Both universities bring great strengths to a large and urgent problem in society. I know we won't solve the spread of extremist hate by ourselves, but I'm confident we can create exciting, effective approaches by collaborating together."

"Before the deadly attack at the Tree of Life synagogue, I rather naively assumed that love always would triumph over hate," said Nordenberg. "As I came to learn more about the powerful tools that are being used to accelerate the spread of hate, however, it seemed clear that in today's world, love needs a helping hand. This center will be positioned to provide badly needed forms of help."

CYLAB RESEARCHERS AWARDED **MURI GRANT TO STUDY HUMAN-BOT TEAMS**

Lujo Bauer, Matt Fredrikson, and Cleotilde Gonzalez are part of a team of researchers that was named a winner of a prestigious US Department of Defense (DoD) Multidisciplinary University Research Initiative (MURI) Award.

(L-R) Lujo Bauer, Matt Fredrikson, and Cleotilde Gonzalez

The team's project aims to address the challenge of human-bot cybersecurity teams (HBCTs), which are commonly deployed to combat cybersecurity threats and attacks but are not yet well understood.

"While we know a lot about how humans use tools to work in teams, little is known about how to manage, observe, and improve hybrid teams that compose of humans and bots," reads the project proposal. "The area of team science that involves human-machine teams is still in its infancy."

Cybersecurity is one of the most challenging tasks that the DoD faces today. A typical human cybersecurity analyst has to deal with a plethora of information, such as intrusion logs, network flows, executables, and provenance information for files. Real-time cybersecurity scenarios are even more challenging: an active adversarial environment consists of large amounts of information and techniques that neither humans nor machines can handle alone.

Machine learning (ML) bots have become part of these cybersecurity teams to reduce the burden on human analysts by filtering information, thus freeing up cognitive resources for tasks related to the high-level mission.

The multi-thrust research project will focus on building robust science on HBCTs, including ways to build trust within these hybrid teams, techniques to focus ML bots on cybersecurity-specific tasks, and methods by which HBCTs integrate information to arrive at decisions. The researchers also plan to study how to coordinate HBCTs in the presence of active adversaries who are also adapting to changing decisions.

The team also consists of researchers from the University of Wisconsin-Madison, University of California-San Diego, Pennsylvania State University, University of Melbourne, Macqurie University, and University of Newcastle. The team brings together diverse expertise spanning computer security, machine learning, psychology, decision sciences, and human-computer interaction.

"The science and engineering challenges we face today are highly complex and often intersect more than one scientific discipline," said Dr. Bindu Nair, director of the Basic Research Office in the Office of the Under Secretary of Defense for Research and Engineering.

"MURIs acknowledge these complexities by supporting teams whose members have diverse sets of expertise as well as creative and different approaches to tackling problems. This cross-fertilization of ideas can accelerate research progress to enable more rapid R&D breakthroughs and hasten the transition of basic research finding to practical application. It's a program that embodies DoD's legacy of scientific impact."

For the FY 2021 competition, the Army Research Office, the Air Force Office of Scientific Research, and the Office of Naval Research solicited proposals in 26 topic areas important to DoD and the Military Services. From a merit-based review of the 298 proposals received, a panel of experts narrowed the proposals to a subset from which the 25 finalists were selected.

Lujo Bauer is a professor in the departments of Electrical and Computer Engineering and the Institute for Software Research (ISR). Matt Fredrikson is an assistant professor in the Computer Science Department and ISR. Cleotilde Gonzalez is a research professor in the department of Social and Decision Sciences.

HOW CYLAB RESEARCHERS ARE **SAFEGUARDING DIGITAL TRANSACTIONS**

In 2013, a Pennsylvania man became the richest person on Earth… for about two minutes. PayPal had accidentally credited his account $92 quadrillion dollars. That's a 92 with 15 zeros behind it. But within minutes, PayPal realized their mistake, and took it all back. Too bad.

Mistakes like this—big, small, and humongous—happen all too often, and typically they come down to bugs in "smart contracts"—computer programs that facilitate digital transactions online. In the case of the PayPal bug: 92 quadrillion is the maximum value that a 64-bit computer can store in its memory. A bug in the code initiated a transfer of funds representing that gigantic number.

As more and more of our finances and purchasing behaviors are moved online, the importance of bug-free smart contracts has never been greater. CyLab's Ankush Das agonizes over this every day.

"If there is a way for a smart contract to accidentally pay you money—if that error exists—somebody will exploit it to pay themselves money. And this happens all the time, all over the place," says Das (shown left), a computer science Ph.D. student advised by CyLab's Jan Hoffman (shown right). "It's very, very important that these smart contracts are free of errors."

Das is the lead designer and developer of a new programming language—which he has named 'Nomos'—aimed at reducing such errors in smart contracts.

"All smart contracts—just like real contracts—have a pre-defined protocol," he says. "Nomos has a way for a programmer to specify what that protocol is. Then, when you're writing the actual program, the language will actually enforce that you satisfy your pre-defined protocol. If you make an error, it will say, 'No no no, this is not correct. There's a protocol mis-match.'"

Another feature of Nomos, Das says, relates to transaction fees the monetary cost of facilitating the transactions themselves. In most scenarios, people rarely pay transaction fees themselves, passing the buck to the credit card companies or the vendors. But on a blockchain—the decentralized network of computers around the world facilitating and recording cryptocurrency transactions—users pay the transaction fee themselves.

> **"It's very very important that these smart contracts are free of errors. People who are skeptical of transacting on certain websites, or paying money in certain portals—the kind of work we are doing can help build people's trust in these systems."**
>
> ***Ankush Das,*** *Ph.D. student, School of Computer Science*

"A cool and unique feature of Nomos is that whenever you write a smart contract, the language will automatically tell you how much the transaction fee will be," says Das. "There's a guarantee—a mathematical theorem running in the background—that says: 'If the language says the fee will be $5,' then it will be exactly $5. Nothing more, nothing less."

Das says that every transaction in the virtual world faces these potential challenges. Blockchains are just the most recent transparent application of smart contracts, exposing these issues to the world. Thus, the research ideas that power Nomos, like ensuring funds are not lost and ensuring protocols are enforced, can be applied in any digital financial realm.

"People who are skeptical of transacting on certain websites, or paying money in certain portals—the kind of work we are doing can help build people's trust in these systems," says Das.

Nomos (nomos-lang.org) is available as a web interface and its code is open-source on GitHub.

THIRD ROUND OF SECURE AND PRIVATE **IoT INITIATIVE FUNDED PROJECTS ANNOUNCED**

Carnegie Mellon CyLab's Secure and Private IoT Initiative (IoT@CyLab) announced its third round of funding, which will support 12 Internet of Things (IoT)-related projects for one year.

While all IoT security and privacy topics are within scope and the focus on Industrial IoT (IIoT) is still central, IoT@CyLab is adding an emphasis on research to help people stay secure as they bring more connected devices into the home as many people continue work from home during the COVID-19 pandemic.

Funding for these projects was made possible by sponsorships from Amazon Web Services, AT&T Business, Cisco, Infineon Technologies, and Nokia Bell Labs. These sponsors were active in working with IoT@CyLab co-directors Anthony Rowe and Vyas Sekar on the request for proposals and proposal review.

"This year we're continuing a focus on IIoT, but we're also revisiting some new, relevant, user-facing concerns as they relate to IoT," Rowe (shown left) and Sekar (shown right) shared in a joint statement.

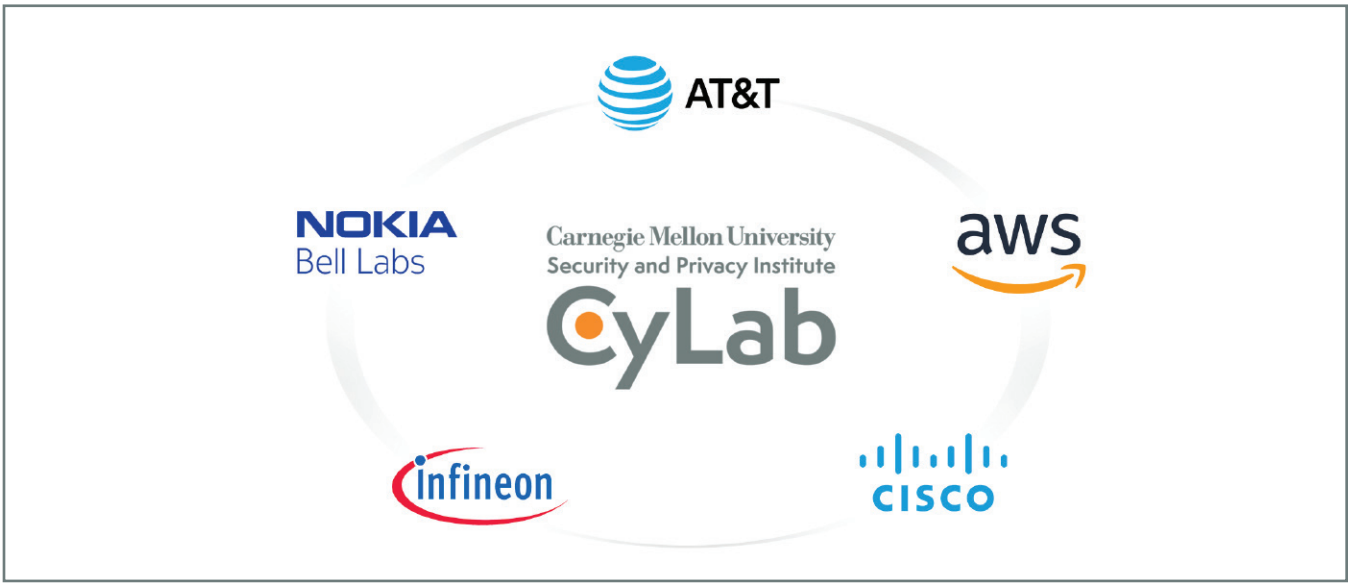
The projects are grouped into three broad research themes: (1) Trustworthy platforms (2) Autonomous healing networks and (3) Accountability. During the execution of these projects, CyLab faculty and students will collaborate with industry sponsors towards the mission of creating the knowledge and capabilities to build secure and privacy-respecting IoT systems. The outcomes from this funding will be presented at the IoT@CyLab annual summit later this year.

The funded projects are listed on page 13.

"This year we're continuing a focus on IIoT, but we're also revisiting some new, relevant, user-facing concerns as they relate to IoT."

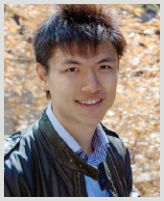
***Anthony Rowe**, Siewiorek and Walker Family Professor, Electrical and Computer Engineering*

***Vyas Sekar**, Tan Family Professor, Electrical and Computer Engineering*



IoT INITIATIVE FUNDED PROJECTS


Heather Miller


Steven Wu


Yuvraj Agarwal


Mayank Goel

Trustworthy platforms

Distributed Data Structures for Federated Learning

- Heather Miller, assistant professor, Institute for Software Research (ISR)

Enabling Privacy-Preserving IoT Apps and Data Analytics

- Steven Wu, assistant professor, ISR
- Yuvraj Agarwal, assistant professor, ISR

Teaching Old Sensors New Tricks to Enable Plug-and-Play Activity Recognition for Opportunistic Health Sensing

- Mayank Goel, assistant professor, Human-Computer Interaction Institute (HCII)

Autonomous healing networks

Systematic Attack Recovery in Industrial Control Systems

- Eunsuk Kang, assistant professor, ISR

Secure, Resilient, and Continuous Machine Learning in Edge Networks

- Osman Yagan, associate research professor, Electrical and Computer Engineering (ECE)
- Soummya Kar, professor, ECE

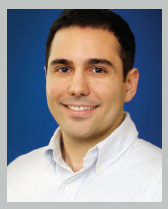
Autonomous Cyber Defense for IIoT using Deductive-Reasoning and Reinforcement Learning

- Ehab Al-Shaer, professor, Information Networking Institute (INI)
- David Garlan, professor, ISR

Oblivious Network Security Analysis using Generative Adversarial Networks

- Giulia Fanti, assistant professor, ECE

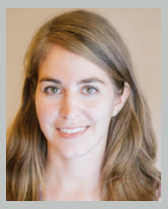

Eunsuk Kang


Osman Yagan

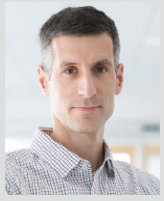

Soummya Kar


Ehab Al-Shaer


David Garlan


Guilia Fanti


Tim Libert


Lujo Bauer


Camille Cobb


Swarun Kumar


Yorie Nakahira

Accountability

Third-Party Network Traffic Attribution for IoT, TV, Web, and Mobile

- Tim Libert, special faculty instructor, ISR

Making smart homes safe for incidental users

- Lujo Bauer, professor, ECE
- Camille Cobb, postdoctoral researcher, CyLab

Robust and explainable ML-based anomaly detection for industrial IoT

- Lujo Bauer, professor, ECE

Wireless Anomaly Detection in Industrial IoT

- Swarun Kumar, assistant professor, ECE

Assuring safety and resilience in affordable IoT systems

- Yorie Nakahira, assistant professor, ECE

For information on how your company can get involved in IoT@CyLab or other security and privacy research at CMU, contact a member of the CyLab partnerships team.

INFERRING WHAT WE SHARE **BY HOW WE SHARE**

A new study by Conrad Tucker shows that patterns in which information is shared online may indicate the information's authenticity.

It's getting harder and harder for humans to decipher real information from fake information online. But patterns in the ways in which information is spread over the Internet—say, from user to user on a social media network—may serve as an indication of whether the information is authentic or not.

Those are the findings of a study by researchers from Carnegie Mellon University's CyLab.

"The challenge with misinformation is that artificial intelligence has advanced to a level where Twitter bots and deepfakes are muddling humans' ability to decipher truth from fiction," says CyLab's Conrad Tucker, a professor of mechanical engineering and the principle investigator of the new study. "Rather than relying on humans to determine whether something is authentic or not, we wanted to see if the network on which information is spread could be used to determine its authenticity."

The study was published in April in Scientific Reports. Tucker's Ph.D. student, Sakthi Prakash, was the study's first author.

"This study has been a long time coming," says Tucker.

To study how real and fake information flows through a social network, studying real Twitter data may seem like the obvious choice. But what the researchers needed was data capturing how people connected, shared, and liked content since the very beginning of a social media network's existence.

"If you look at Twitter right now, you'd be looking at an instant in time when people have already connected," says Tucker. "We wanted to look at the beginning—at the start of a network—at data that is difficult to attain if you're not the owner or creator of the platform."

Because of these constraints, the researchers built a Twitter-like social media network and asked study participants to use it for two days. The researchers populated the social network with 20 authentic and 20 fake videos, collected from verified sources of each, but users were not aware of the authenticity of the videos. Then, over the course of 48 hours, 620 participants joined, began following each other, shared and liked the videos on this simulated social media network.

To encourage participation, study participants were incentivized: the user with the most followers at the end of the two-day study was awarded a $100 cash prize. However, all users were given a credibility score that everyone on the network could see. If users shared too much content that the researchers knew was fake, their credibility score would take a hit.

This simulated Twitter-like social media network is the first of its kind, Tucker says, and is open-sourced for other researchers to use for their own purposes.

"Our goal was to derive a relationship between user credibility, post likes, and the probability of one user establishing a connection with another user," says Tucker.

It turns out, this relationship would prove useful in inferring whether or not misinformation is being shared on a particular social media network, even if the content itself being shared is unknown. In other words, the patterns in which information is shared across a network—with whom it is shared, the amount of likes it receives, etc.—can be used to infer the information's authenticity.

"Now, rather than relying on humans themselves to identify misinformation, we may be able to rely on the network of humans, even if we don't know what they are sharing," says Tucker. "By looking at the way in which information is being shared, we can begin to infer what is being shared.

"As the world advances towards more cyber-physical systems, quantifying the veracity of information is going to be critical," says Tucker.

Given that current mechanical systems are becoming more connected, Tucker highlights the opportunity for mechanical engineering researchers to play a critical role in understanding how the systems that they create impact people, places, and policy.

"We had mechanical systems that evolved to electro-mechanical, then to systems that collect data," says Tucker. "Since people are part of this network, you have people who interact with these systems, and you have asocial science component of that, and we need to understand these vulnerabilities as it relates to our mechanical and engineering systems."

PICOCTF ANNOUNCES
2021 COMPETITION WINNERS

picoCTF, which over the course of nearly a decade has become the world's largest online hacking competition, held its 2021 competition last spring. Nearly 15,000 people from over 130 countries around the world competed in the annual two-week competition, which ran March 16-30.

"The skills taught in this competition are essential not only to future cybersecurity professionals, but to anyone living in today's digital society," said CyLab's Hanan Hibshi, assistant teaching professor in the Information Networking Institute and a faculty advisor to picoCTF. "This competition has given thousands of people a fun and approachable way to learn and hone their cybersecurity skillset."

During the two-week competition, participants were tasked with solving up to 88 cybersecurity challenges. Those challenges, designed to mimic real-life cybersecurity problems, were created by Carnegie Mellon's internationally-acclaimed competitive hacking team, the Plaid Parliament of Pwning.

Challenges started off easy, allowing students with little or no experience to get started, but gradually increased in difficulty, eventually testing even the most experienced hackers. If participants became stuck, they could access nuggets of clues on how to solve a particular challenge or attempt similar challenges in the picoGym, the non-competitive environment within the picoCTF platform where users practice various cybersecurity skills.

> **"This competition has given thousands of people a fun and approachable way to learn and hone their cybersecurity skillset."**
>
> ***Hanan Hibshi,*** *assistant teaching professor in the Information Networking Institute and a faculty advisor to picoCTF*

The challenges themselves were housed in an outer space-themed video game with a unique storyline, designed by students in Carnegie Mellon's Entertainment Technology Center Opens in new window. Solving particular challenges unlocked other parts of the game's virtual world.

Prizes were awarded to the top 10 US-based middle and high school teams.

This year's top 10 teams consisted of players from California, Colorado, Maryland, New Jersey, Ohio, Pennsylvania, Texas, Utah, Virginia, Washington, and West Virginia. The winning team, "lightgoldenrodyellowpwn," solved all 88 challenges over the course of 1 day, 9 hours.

CRYPTOCURRENCY DERIVATIVES MARKETS ARE BOOMING

A first-of-its-kind study by Carnegie Mellon University CyLab researchers shows just how incredibly popular crypto derivatives markets are.

Markets for cryptocurrency derivatives—contractual side-bets on the future price of cryptocurrencies—have exploded in recent years. On a busy day, over $100 billion in these derivatives are traded, rivaling the daily volume traded in the New York Stock Exchange. What's more, there is evidence that the activity inside these markets may affect the value of cryptocurrencies themselves.

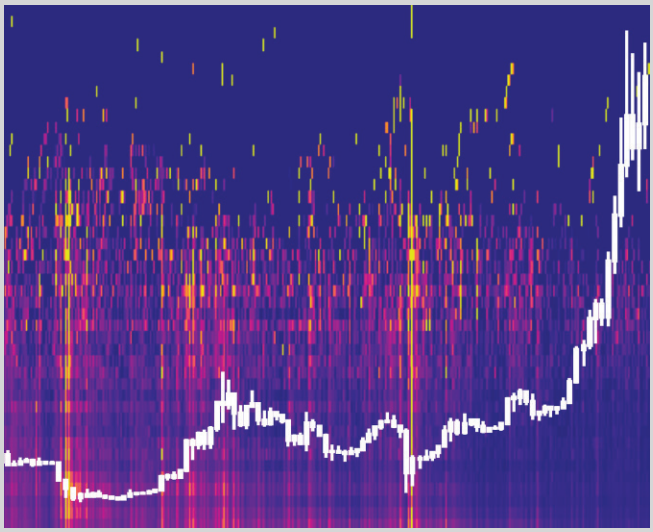
These are a few of the findings of a first-of-its kind study by Carnegie Mellon University CyLab researchers, which were presented at the The Web Conference in April.

"On average, the traded volume in cryptocurrency derivatives markets exceeds the regular crypto spot markets by a factor of five," says CyLab's Kyle Soska, a Ph.D. student in electrical and computer engineering and the study's lead author.

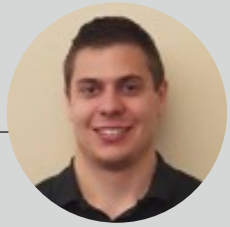
In their study, the researchers performed a comprehensive analysis of BitMEX, a derivatives exchange that initially launched in 2014 and would become one of most successful exchanges by volume traded. Performing analyses on publicly-available data from BitMEX, the researchers were able to put together the first comprehensive look into the massive amounts of activities that occur in these types of markets.

As a companion to their study, the researchers built and released a public website that provides a live record of BitMEX and provides real-time access to their analysis platform for other researchers, economists, and interested parties.

"Derivative markets are important because their behavior influences the price dynamics of cryptocurrencies themselves," says CyLab's Nicolas Christin, a co-author of the study and a professor in the Institute for Software Research (ISR) and Department of Engineering and Public Policy (EPP).



> **"The traded volume in cryptocurrency derivatives markets exceeds the regular crypto spot markets by a factor of five."**
>
> ***Kyle Soska,*** *Ph.D. student, Electrical and Computer Engineering*



Christin describes this as a bit like a chicken-and-egg problem. People could use derivative markets to hedge against certain price movements, he says, but in turn, derivative markets with high leverage may create instability cycles: volatility in cryptocurrency prices then causes more liquidations in derivative markets, which results in volatile cryptocurrency prices.

An analysis of archived messages in BitMEX's site-wide chat room illustrates a highly diverse population of traders. Most interestingly, messages in Korean—the vast majority presumably originating in Korea, which encompasses a single time zone—were almost time-invariant. In other words, while one would expect activity to occur during normal "daytime" hours, the chat analysis suggests that a large population of Korean traders were active 24/7.

"There's this quote, 'Money never sleeps,'" says Christin. "... But Wall Street mainly trades between 9:30 a.m. and 4 p.m. In these cryptocurrency derivatives markets, we see data that show people in the same time-zone trading every minute of the day."

Trading on BitMEX and other cryptocurrency derivatives markets is a high-risk, high-reward endeavor. First, traders can use what's referred to as "leverage," meaning that they can wager a much larger bet—commit to a much larger position—than they can cover with the funds currently in their account. This can yield huge wins, but also immediate losses.

Adding to the risk is the fact that unlike traditional currency markets, all one needs to trade on cryptocurrency derivatives platforms is a valid email address, some cash, and a few minutes' time.

"Our data show really small positions in these markets—likely held by people with not a ton of experience—being disproportionately liquidated," says Soska. "Our findings suggest a familiar story in a relatively new and burgeoning market: that really sophisticated people show up and have a significant edge over amateurs."

Looking forward, Christin says that cryptocurrency derivative markets are beginning to dwarf normal markets, and this affects not just those steeped in the crypto world, but even those outside of it.

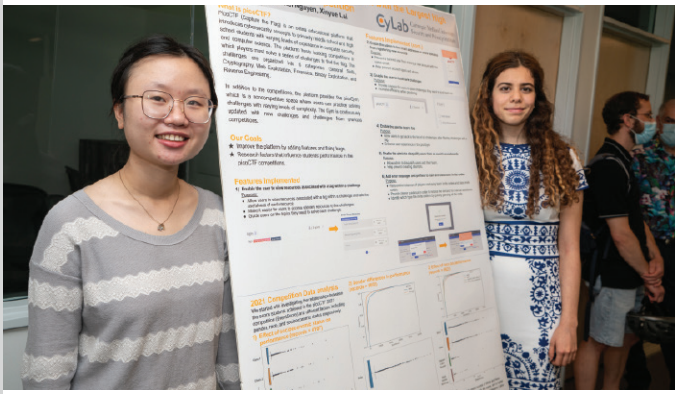
"These markets are becoming more mainstream, whether we like it or not," Christin says. "Even if you personally aren't interested in cryptocurrencies, it's possible your financial advisor or a firm trading on your behalf will be soon."

This study was a collaboration between researchers at three different colleges at Carnegie Mellon University—the College of Engineering, the School of Computer Science, and the Tepper School of Business.

> **"Derivative markets are important because their behavior influences the price dynamics of cryptocurrencies themselves."**
>
> ***Nicolas Christin,*** *professor in the Institute for Software Research (ISR) and Department of Engineering and Public Policy (EPP)*

Undergrads from around the nation partake in CyLab research

Each year, dozens of undergraduate students enrolled at CMU and other colleges and universities around the nation participate in CMU's Research Experience for Undergraduates (REU), a program that gives undergraduate students real-life experience in scientific research. This year, several CyLab faculty took students in this year's REU class under their wings to pursue research pertaining to security and privacy. The REU students presented their research at a poster session at the conclusion of the program.



PHISHING, FAIRNESS, AND MORE: **CYLAB'S 2021 SEED FUNDING AWARDEES**

Over $350K in seed funding has been awarded to 14 different faculty and staff in seven different departments across three colleges at CMU. Funding was awarded based on the projects' intellectual merit, originality, fit towards CyLab's priorities, and potential impact.

"We're excited to help seed and continue some exciting security and privacy research projects being conducted by faculty across the university," said CyLab director Lorrie Cranor.

The awards selection committee, made up of CyLab-affiliated faculty and representatives from partner organizations, prioritized the following aspects in no particular order when making their selections:

- Collaboration between CyLab faculty in multiple departments
- Projects led by or having significant involvement of junior faculty
- Seed projects that are good candidates for follow-on funding from government or industry sources
- Projects that are making good progress but reaching the end of their previous funding and need funding to finish or to continue the project until other sources of funding are obtained
- Efforts to transition research to practice, e.g. by preparing software for release as open source projects, conducting field trials, or deploying research results in real-world applications
- Projects that can get started quickly and make significant progress with a small amount of funding
- Non-traditional projects that may be difficult to fund through other sources
- Education or outreach projects aimed at broadening participation in the security and privacy field

Recipients of the awards will be required to submit brief quarterly reports outlining the progress of the project and present a talk or poster at the annual CyLab Partners Conference this Fall.

Updating Estimates of the Value of Time to Read Privacy Policies

- *Aleecia McDonald* (shown right), Assistant Professor of the Practice, Information Networking Institute (INI)

Secure Software Evolution

- *Rohan Padhye,* assistant professor, Institute for Software Research (ISR)

Exploit Synthesis for Node.js Packages

- *Limin Jia,* Associate Research Professor, Electrical and Computer Engineering (ECE)

- *Ruben Martins* (shown left), Systems Scientist, Computer Science Department

Personalized Phishing Detection Training using Cognitive Models

- *Drew Cranford,* Postdoctoral Researcher, Department of Psychology
- *Coty Gonzalez,* Research Professor, Social and Decision Sciences (SDS)
- *Christian Lebiere,* Research Psychologist, Department of Psychology
- *Palvi Aggarwal,* Postdoctoral Fellow, SDS
- *Kuldeep Singh,* Systems Software Associate, SDS

FedAtk: Interference Attacks on Personalized Learning Models

- *Carlee Joe-Wong* (shown right), Assistant Professor, ECE

User-facing Analytics and Management of Consumer IoT Security

- *Patrick Tague,* Associate Teaching Professor, INI

Evaluating the Impact of Communication Disruption on Vehicle to Grid Technologies

- *Amritanshu Pandey,* Systems Scientist, ECE
- *Lawrence Pileggi,* Professor and Department Head, ECE

On the Impact of Algorithmic Fairness Metrics and Methods on Trust in Machine Learning Systems

- *Hoda Heidari,* Assistant Professor, Machine Learning Department & ISR

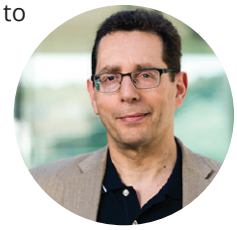
CMU LAUNCHES **NEW PRIVACY ENGINEERING OPTIONS**

Two new options make it easier for working professionals to receive privacy engineering training.

As new privacy regulations like the General Data Protection Regulation and the California Consumer Privacy Act require companies to improve the way they handle user privacy, more and more working professionals are seeking formal training in privacy engineering.

"While we've offered a full-time Master's degree program in privacy engineering since 2013, until now we haven't had an option for those seeking privacy engineering training while continuing to work," says CyLab's Lorrie Cranor, co-director of CMU's Privacy Engineering Program and a professor in the Institute for Software Research and the department of Engineering and Public Policy.

Now, CMU is offering two flexible options for privacy engineering education and training. The first will allow working professionals to pursue the Master of Science in Information Technology - Privacy Engineering (MSIT-PE) degree part-time and remotely. Depending on the number of courses taken per semester, the part-time degree program can be completed in between two and four years.



"Working professionals no longer need to quit their jobs and move to Pittsburgh to pursue this degree and receive the training they need," says CyLab's Norman Sadeh, co-director of CMU's Privacy Engineering Program and a professor of computer science in the Institute for Software Research.

For working professionals who aren't able to commit to a part-time Master's degree program, CMU is now offering an additional option: a privacy engineering certificate that can also be obtained remotely. The certificate program comprises a combination of mini-tutorials, class discussions, and hands-on exercises aimed at delivering the fundamentals of privacy engineering.

Carnegie Mellon University privacy ENGINEERING

"The idea behind the privacy engineering certificate is that working professionals can learn the key concepts in privacy engineering on the weekend over the course of just a few weeks," says Sadeh.

The certificate program is available to individual students as well as cohorts of 15-25 students from a single organization.

According to the International Association of Privacy Professionals, Privacy Engineers in the U.S. earn an average salary of $136,000. Those with a Privacy Technologist certification earn over $170,000.

"Graduates from our privacy engineering programs will be well-equipped to compete in this emerging, fast-growing job market," says Cranor.

To learn more about the part-time MSIT-PE program, visit the Privacy Engineering Program website.

To learn more about the privacy engineering certificate program, visit the Privacy Engineering Certificate page.

> **"Working professionals no longer need to quit their jobs and move to Pittsburgh to pursue this degree and receive the training they need."**
>
> ***Norman Sadeh**, co-director, Privacy Engineering Program*

SECURITY AND PRIVACY DEGREE PROGRAMS OFFERED AT CMU

Security and privacy courses and degree programs are offered across many departments at Carnegie Mellon and include courses for both undergraduate and graduate students. We offer courses for computer science and engineering students, as well as courses suitable for policy and management students. Both full-time and part-time programs are available, with new programs being added this year.

New this year: online security and privacy course listing

For the first time ever, CMU students can browse all security and privacy courses offered at the University in one centralized location: the CyLab website. Users may sort the courses by course number, name, semester offered, and more for ease of navigation and read course descriptions, access syllabi, and learn about any pre-requisites, among other information. The course listing can be found at www.cylab.cmu.edu/education/courses.html.

Undergraduate Minor in Information Security, Privacy, and Policy

The Undergraduate Minor in Information Security, Privacy, and Policy offers undergraduate students from any major an opportunity to take a deep dive into policy issues related to security and privacy. The program is offered jointly by the Institute for Software Research (ISR) and Engineering and Public Policy (EPP).

Undergraduate Concentration in Security & Privacy

The Security & Privacy concentration for undergraduate students is designed to expose both Electrical and Computer Engineering (ECE) and Computer Science students to the key facets of and concerns about computer security and privacy that drive practice, research, and legislation. On completing the curriculum, students will be well prepared to continue developing their interests in security or privacy through graduate study; to take jobs in security or privacy that will provide further training in applicable areas; and to be informed participants in public and other processes that shape how organizations and society develop to meet new challenges related to computer security or privacy.

One can now browse all of CMU's security and privacy course offerings in one centralized location on the CyLab website.

Master's Programs

- The Master of Science in Information Security (MSIS) degree, offered in the College of Engineering's Information Networking Institute (INI), offers a technical focus in security and computer systems, further developed through research opportunities. Graduates may pursue doctoral degrees or obtain positions as security experts equipped to manage the emerging complexities associated with securing data, networks and systems.
- The Master of Science in Information Technology - Privacy Engineering (MSIT-PE) degree, offered in the School of Computer Science's Institute for Software Research, is a 12- or 16-month graduate program for computer scientists and engineers who wish to pursue careers as privacy engineers or technical privacy managers. A part-time option is also available.
- The Master of Science in Information Security Policy and Management (MSISPM), offered in Heinz College, provides students with background and insights into general and technical coverage of information security, while equipping them with the analytical methods and management practices necessary to succeed as managers in the field of information security.

Ph.D. Programs

While there is no Ph.D. program at CMU dedicated specifically to security and privacy, students in several programs focus their research on security and privacy.

- Ph.D. programs in the School of Computer Science where some students focus on security and privacy include Human-Computer Interaction, Language Technologies, Machine Learning, Software Engineering, Computer Science, and Societal Computing.
- Ph.D. programs in the College of Engineering where some students focus on security and privacy include ECE and EPP.

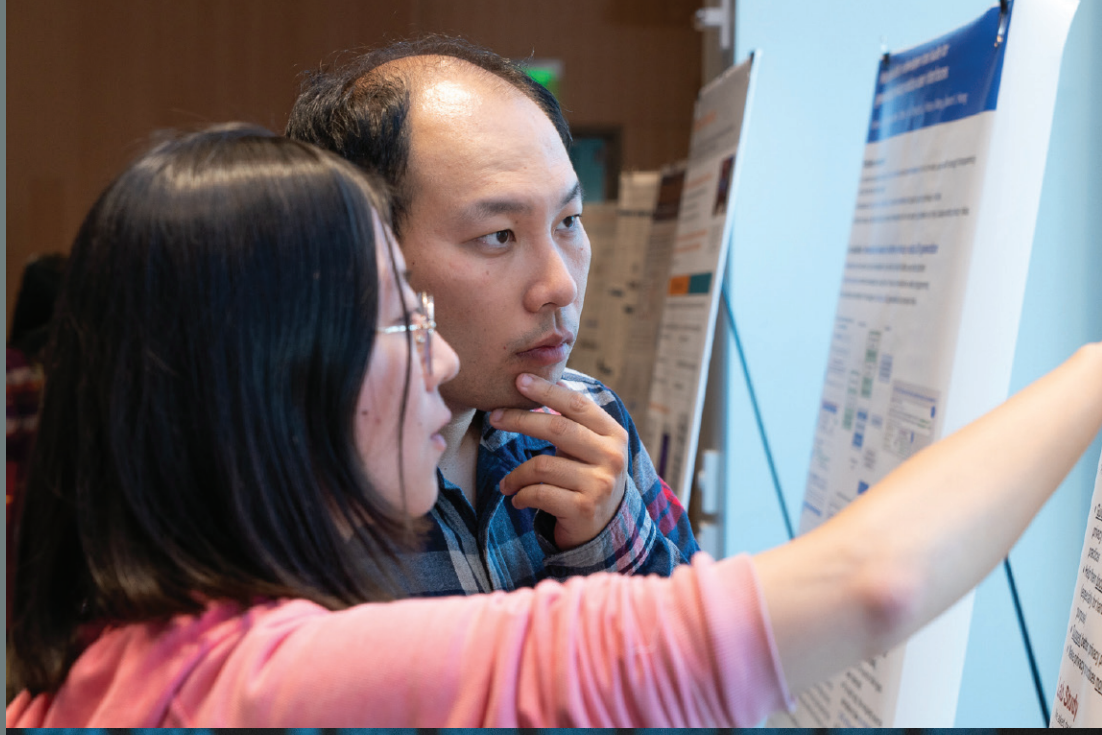
CyLab Executive Education Offerings

The rapidly evolving landscape of technology-related security and privacy challenges requires an understanding of the business application and the ability to apply best practices to create solutions. From open enrollment to bespoke training programs, CyLab educators and researchers will empower you and your organization to solve critical challenges.

CyLab offers training in these topics and more:

- Artificial Intelligence (AI), Machine Learning, Security and Privacy
- Behavioral Cybersecurity
- Biometrics and AI
- Blockchain and Cryptography
- Cyber Workforce Development
- Darkweb, Security Economics, Crime, and Fraud
- Ethical Issues in AI & Cybersecurity
- Internet of Things (IoT) Connected Products Security and Privacy
- Privacy Engineering
- Social Cybersecurity and Social Network Analysis
- Software-Defined Security for Next Generation Networks
- Usable Privacy and Security

Interested in learning more about these offerings or designing your own program? Contact the CyLab partnerships team (partnerships@cylab.cmu.edu) to learn more.



YINGLIAN XIE RECEIVES 2021 CYLAB ALUMNI AWARD

Yinglian Xie, a CyLab alum and co-founder and CEO of DataVisor, has been selected to receive the 2021 CyLab Distinguished Alumni Award as "one of the pioneers in the space of operationalizing the application of advanced machine learning techniques applied to pressing security problems faced by enterprises across the entire industry landscape," according to the award. The award honors CyLab alumni from any CMU department who have had impactful achievements related in the fields of security and/or privacy.

"I am very honored to receive this award," says Xie. "I thank CMU and CyLab for the experience and for setting the foundation for my love of security topics."

The award will be presented to Xie at the 2021 CyLab Partners Conference in October.

"Yinglian's work in security analytics and fraud management has advanced the state of art both in theory and perhaps more importantly in practice in this domain," says CyLab's Vyas Sekar, a professor of Electrical and Computer Engineering who nominated Xie for the Award. "In many ways, her early research at CMU and beyond was well ahead of its time and serves as the intellectual forerunner of today's flourishing array of products on applying 'big data' analytics to security problems."

Xie was a computer science Ph.D. student at CMU during the birth of CyLab. She began her studies in 1999, co-advised by David O'Halloran and Hui Zhang, and later collaborated closely with CyLab's Mike Reiter who served on her Ph.D. committee. After graduation, Xie worked with Reiter as a postdoctoral researcher from 2005-2006.

Her Ph.D. thesis, "A Spatiotemporal Event Correlation Approach to Computer Security," explored a new approach to detect abnormal patterns of a wide range of cyberattacks, whose network patterns—when observed individually—may not seem suspicious or distinguishable from normal activity changes.

> **"CMU encourages not just research but the impact that research could have. I really wanted something generating impact to the industry and bridge the gap between research and what is out there for everyone's day to day work."**
>
> ***Yinglian Xie,*** *CyLab alum and co-founder / CEO of DataVisor*

"My thesis set the theme for all of my work, which is about data-driven approaches to security," Xie says. "If you put all data together in one place, you can do very powerful things in security."

After her time at CMU, Xie worked at Microsoft Research for seven years, continuing to pursue new and innovative ways improve security and privacy using data-driven approaches. At Microsoft, she began to explore machine learning and what's known as parallel computing—the breaking down of larger computational problems into smaller parts that can be executed simultaneously on multiple computer processors.

"We wanted to know, what are the newer things that we couldn't do in the past that we could do now with these newer capabilities?" Xie says.

Then, in 2013, she co-founded DataVisor, a security company that uses the similar research themes and principals that Xie had been pursuing at Microsoft and CMU. DataVisor provides "the world's most sophisticated AI-powered solutions to keep companies and their customers safe from fraud and abuse," according to the company's website. Protecting over four billion user accounts worldwide, DataVisor enables leading financial institutions, banks and online properties manage fraud and risk at enterprise scale.

"We demonstrated to the industry, and we were the first in the market to handle billions of events and transactions in real time doing unsupervised machine learning to discover new and novel attacks," Xie says.

Xie says that she wouldn't be where she is today without her experience at CMU.

"CMU encourages not just research but the impact that research could have," she says. "I really wanted something generating impact to the industry and bridge the gap between research and what is out there for everyone's day to day work."

2020-2021 Graduated Ph.D. Students

João Antunes, Ph.D. in Electrical and Computer Engineering (ECE)
Advisors: Asim Smailagic and Dan Siewiorek
Thesis: *Leveraging Context for Multi-Lable Action Recognition and Detection in Video*
Defense: July 2020

Mihovil Bartulović, Ph.D. in ECE
Advisor: Kathleen Carley
Thesis: *On Trail Comparison, Clustering, and Prediction: Building a Framework for Working With Sequential Network Data*
Defense: April 2021

Iain Cruikshank, Ph.D. in the Institute for Software Research (ISR)
Advisor: Kathleen Carley
Thesis: *Multi-view Clustering of Social-based Data*
Defense: July 2020

Sanghamitra Dutta, Ph.D in ECE
Advisor: Pulkit Grover
Thesis: *Strategies for Fair, Explainable, and Reliable Machine Learning Using Information Theory*
Defense: April 2021
Current position: JP Morgan Chase research until April 2022, after which she will join the ECE department at the University of Maryland College Park as tenure-track faculty.

Madhumitha Harishankar, Ph.D. in ECE
Advisors: Patrick Tague and Carlee Joe-Wong
Thesis: *Incentivizing User-centric Resource Allocation in Wireless Networks in Realtime*
Defense: December 2020

Cody Kinneer, Ph.D. in ISR
Advisors: David Garlan and Claire Le Goues
Thesis: *Search-based Plan Reuse in Self-* Systems*
Defense: May 2021

Min Hun Lee, Ph.D. in ECE
Advisors: Asim Smailagic and Dan Siewiorek
Thesis: *Interactive Hybrid Intelligence Systems for Human – AI/Robot Collaboration*
Defense: July 2021

Kyle Soska, Ph.D. in ECE
Advisor: Nicolas Christin
Thesis: *Security Defender Advantages via Economically Rational Attacker Modeling*
Defense: May 2021
Current position: Now a postdoc at CMU

Janos Szurdi, Ph.D. student in ECE
Advisor: Nicolas Christin
Thesis: *Empirically Analyzing and Combating the Malicious Utilization of Domain Names*
Defense: August 2020
Current position: Palo Alto Networks

Josh Tan, Ph.D. in Societal Computing
Advisors: Lorrie Cranor and Lujo Bauer
Thesis: *Practical Security Guidance for Authentication-System Designers*
Defense: September 2020
Current position: Amazon

Aman Tyagi, Ph.D. in Engineering and Public Policy (EPP)
Advisor: Kathleen Carley
Thesis: *Challenges in Climate Change Communication on Social Media*
Defense: February 2021

Samuel Yeom, Ph.D. in Computer Science
Advisor: Matt Fredrikson
Thesis: *Black-Box Approaches to Fair Machine Learning*
Defense: June 2021

Diana Zhang, Ph.D. in ECE
Advisor: Swarun Kumar
Thesis: *Exploring Novel Sensing Paradigms for Existing Wireless Infrastructure*
Defense: June 2020
Current position: Johns Hopkins University – Applied Physics Laboratory

CyLab Names 2021 Presidential Fellows

Since 2014, CyLab has recognized high-achieving Ph.D. students pursuing security and/or privacy-related research with a CyLab Presidential Fellowship. Fellowships cover one year of tuition.

"The committee had a hard time deciding among many extremely qualified students this year," says CyLab's Nicolas Christin, who chaired this year's selection committee. "The fellows that were selected represent the best of the best Carnegie Mellon, and CyLab, have to offer, and we are fortunate to have them here."

In addition to Christin, this year's selection committee included Giulia Fanti, Corina Pasareanu, and Rohan Padhye.

This year's CyLab Presidential Fellowship recipients are:

Nirav Atre

Ph.D. student in the Computer Science Department (CSD), advised by CSD professor Justine Sherry

Atre's research focuses on a class of cyberattacks known as algorithmic complexity attacks (ACAs). When a malicious hacker deploys an ACA, they send traffic that is designed to be extremely expensive to process, bringing computer servers to a crawl and ruining the browsing experience for regular users. Atre is working to develop general techniques to protect vulnerable network deployments from the debilitating impact of ACAs.

Denial-of-Service (DoS) attacks such as ACAs are purported to cost the industry upwards of $10 billion per year in lost revenue and operational expenses.

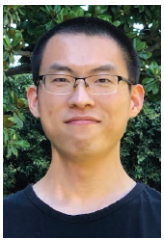
"This fellowship will support my efforts to implement practical defenses against such attacks, to shield service providers from the associated costs, and to ensure that users experience uninterrupted service," says Atre.

Tianshi Li

Ph.D. student in the Human-Computer Interaction Institute (HCII), advised by HCII professor Jason Hong

Li's research focuses on helping developers make privacy-friendly apps. She's particularly interested in understanding why developers create apps that violate users' expectations of privacy and building developer tools to make protecting users' privacy an easier task.

"Most developers are not privacy experts, while they have little support to comply with the ever-growing privacy requirements," says Li. "This fellowship will help me continue exploring the design space of developer tools for privacy and release the tools I built to benefit real-world developers and their users."

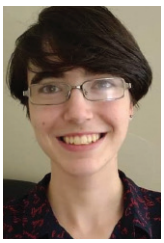


Yifan Song

Ph.D. student in CSD, advised by CSD professor Vipul Goyal

Song's research focuses on the notion of multi-party computation (MPC), which allows several mutually distrusted parties to compute a common function while protecting the privacy of their inputs. MPC is a powerful tool to solve the privacy issue and has many applications in the real world, such as distributed voting and private bidding and auctions. Song aims to improve the concrete efficiency of MPC to make it more practical for real world applications.

"I feel very honored to be selected as one of the CyLab Presidential Fellows," Song says. "This fellowship represents as a recognition of my previous achievements and my future plans, and it will encourage me to continue doing research along the line of efficient MPC."



Milijana Surbatovich

Ph.D. student in Electrical and Computer Engineering (ECE), advised by ECE professors Limin Jia and Brandon Lucia

Surbatovich's research focuses on intermittently-powered energy-harvesting devices, which are devices that do not need battery maintenance, instead operating only when energy is available to harvest and thus frequently turning on and off. While maintenance freedom enables these devices to be deployed in exciting new environments—such as in tiny-satellites or smart city sensing—this intermittent operational cycle makes proving necessary software correctness and security properties difficult. Her research aims to provide both formal models of correctness properties and the runtime systems that guarantee these properties.

"The support from this fellowship will allow me to pursue my research in operationalizing formal correctness reasoning to provide practical tools and systems that programmers can use to guarantee that their intermittent-computing applications will run correctly and securely," Surbatovich says.

CYLAB **SEMINAR SERIES**

Each year, CyLab holds a seminar series in the Fall and Spring semesters, bringing security and privacy experts together to share their research with the CyLab community. Here are the speakers we have featured in the past year.

September 14, 2020
Gianluca Stringhini

Assistant professor, Boston University
Title: Computational Methods to Measure and Mitigate Weaponized Online Information

September 28, 2020
Cecilia Testart

Ph.D. Candidate in EECS, MIT CSAIL
Title: Towards data-driven Internet routing security

October 5, 2020
Bruno Biais

Professor, HEC Paris
Title: Equilibrium Bitcoin Pricing

October 12, 2020
Mike Specter

Ph.D. Candidate, MIT CSAIL
Title: Security and Privacy of U.S. Deployed Internet Voting Systems

October 26, 2020
Christopher Kiekintveld

Associate Professor, University of Texas at El Paso
Title: Challenges and Opportunities in AI for Cyber Security and Cyber Deception

November 2, 2020
Mike Reiter

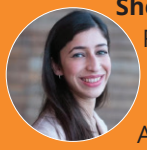
Professor, University of North Carolina at Chapel Hill
Title: Leveraging Cross-Website Coordination to Mitigate Credential Stuffing

November 9, 2020
Silvio Micali

Professor, MIT & Founder of Algorand
Title: Algorand – The Truly Distributed Blockchain

November 16, 2020
Seny Kamara

Professor, Brown University
Title: Crypto for the People

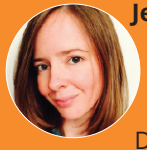
December 7, 2020
Shehar Bano

Research Scientist, Facebook
Title: Twins: White-Glove Approach for BFT Testing

March 8, 2021
Greg Shannon

Chief Scientist, SEI CERT Division
Title: CyManII

March 15, 2021
Christina Pöpper

Assistant Professor of Computer Science, NYU Abu Dhabi
Title: High we Fly: Wireless Witnessing and Crowdsourcing for Air-traffic Communication Security

March 22, 2021
Jessica Vitak

Associate Professor, University of Maryland
Title: Connecting Contexts: Designing Privacy and Security Resources to Teach Core Concepts to Children and Families

March 29, 2021
Carmela Troncoso

Assistant Professor, EPFL
Title: Designing technology in pandemic times

April 12, 2021
Adrian Perrig

Professor, ETH Zurich; CyLab Fellow and former Technical Director
Title: Experiencing a New Internet Architecture

April 19, 2021
Ewa Syta

Assistant Professor of Computer Science, Trinity College
Title: CALYPSO: Private Data Management for Decentralized Ledgers

April 26, 2021
Srini Devadas

Professor, MIT CSAIL
Title: Data Augmentation and Uniform Transformation for Learning with Scalability and Security

May 3, 2021
Alice Hutchings

Deputy-Director, Cambridge Cybercrime Centre
Title: Lights! Camera! Action! Using crime script analysis for cybercrime prevention

FEATURED SPEAKING ENGAGEMENTS
BY FACULTY

Alessandro Acquisti

- "The Impact of the GDPR on Content Providers." Keynote talk, Conference on Artificial Intelligence, Machine Learning, and Business Analytics. *December 2020.*
- Opening of the Academic Year Invited Speech. BA in Global Governance, Department of Economics and Finance, University of Rome Tor Vergata. *September 2020.*

Stephanie Balzer

- "Session Logical Relations for Noninterference." Invited talk, 27th International Conference on Types for Proofs and Programs. *June 2021.*
- Invited lecturer. Oregon Programming Languages Summer School. *June 2021.*

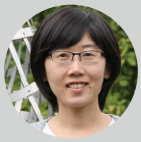
Lujo Bauer

- "On evasion attacks against machine learning in practical settings." Keynote talk, 49th Annual IEEE AIPR: Trusted Computing, Privacy, and Security Multimedia. *October 2020.*
- "On the practical risks and benefits of AI to security." Keynote talk, 5th Italian Conference on Cybersecurity. *April 2021.*
- "Beyond l_p balls: Attacks on real-world uses of machine learning." Workshop on Adversarial Machine Learning in Real-World Computer Vision Systems. *June 2021.*

Kathleen Carley

- "Disinformation and Manipulation during COVID-19 & the Election." Keynote talk, Statistical and Applied Mathematical Sciences Institute Conference. *May 2021.*
- "The Power of High Dimensional Networks." Keynote talk, North American Social Network (NASN). *January 2021.*
- "Disinfodemic." Keynote talk, McGowan Symposium on Business Leadership and Ethics. *October 2020.*
- "Disinformation Playground for Bots and Trolls." Keynote talk, Social Threats in Challenging Times: How Families and Other Human Systems Adapt, 41st Pittsburgh Family Systems Conference and Symposium. *October 2020.*
- "Social Cybersecurity and the Pandemic." Keynote talk, International AAAI Conference on Web and Social Media. *June 2020.*

Yuejie Chi



- "Nonconvex Low-Rank Matrix Estimation: Geometry, Robustness, and Acceleration." Plenary Speaker, SIAM Conference on Imaging Science. *July 2020.*

Nicolas Christin

- "A deep dive in the deep web: Insights from eight years of online anonymous marketplaces measurements." MIT Lincoln Lab. *July 2020.*
- "The dark web isn't that dark." United Nations Office of Drug and Crime. 52nd session of the United Nations Statistical Commission, Side Event. *February 2021.*
- "Cryptocurrency trading at 10: From "Monopoly money" to billion-dollar derivatives markets. Invited talk. University College London. London, UK. *June 2021.*

Lorrie Cranor

- Keynote talk, "Keeping it real and accounting for risk: usable privacy and security study challenges." Human Factors and Ergonomics Society 64th International Annual Meeting (HFES2020). *October 2020.*
- Keynote talk, "Useful and Usable Privacy Interfaces." Workshop on AI for Privacy (AI4P), 24th European Conference on Artificial Intelligence. *September 2020.*
- "Illustrating Privacy Engineering Concepts with Potty Talk." USENIX Privacy Engineering Practice and Respect Conference. *June 2021.*

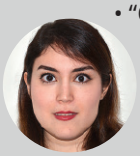
Matthew Fredrikson

- "How to find ML bugs that expose training data and bias outcomes." Keynote talk, DeepTest. *July 2020.*
- Invited speaker. University of Wisconsin-Madison Programming Languages Seminar. *October 2020.*

David Garlan

- "Reflections on the Role of Software Architecture in Software Engineering Education." Keynote talk, Joint Track on Software Engineering Education and Training, 43rd International Conference on Software Engineering. *May 2021.*

Hoda Heidari



- "On the Meaning and Limitations of Mathematical Formulations of Fairness." Artificial Intelligence Conference hosted by Duke-Kunshan University. *November 2020.*
- "Algorithmic Fairness through the Lens of Causality and Interpretability." Virtual NeurIPS 2020 Workshop. *December 2020.*
- "AI Bias and (Un)Fairness." Max Planck Symposium on Computing and Society. *January 2021.*
- "On Modeling Human Perceptions of Allocation Policies with Uncertain Outcomes." Foundations of Algorithmic Fairness Workshop. *March 2021.*

Hanan Hibshi

- "picoCTF." International Visitor Leadership Program's Cybersecurity and Safe Digitization project for Switzerland. *March 2021.*

Limin Jia

- "Connecting Information Flow Types to Runtime Monitors via Gradual Typing." Invited talk, 48th ACM SIGPLAN Symposium on Principles of Programming Languages. *January 2021.*
- "(Bridging) the gap between formal information flow security analysis and real-world applications." Invited talk, 34th IEEE Computer Security Foundations Symposium. *June 2021.*

Jon Peha

- "Spectrum for Intelligent Transportation Systems." United Nations' International Telecommunications Union. *December 2020.*

Norman Sadeh

- "Design of a Privacy Infrastructure for the Internet of Things." USENIX Privacy Engineering Practice and Respect Conference. *October 2020.*

Mark Sherman

- "Transfer Learning Applications and Deep Fake Videos." Ai4 2021 Cybersecurity Summit. *February 2021.*
- "Threats to Machine Learning Applications." Strategic Deterrence Digital Engineering Conference at the Johns Hopkins University Applied Physics Lab. *November 2020.*
- "Threats to Transfer Learning Applications." Workshop on Naval Applications of Machine Learning. *March 2021.*

Carol Smith

- "Embrace Ethics to Make Trustworthy Tech." IEEE Women in Engineering International Leadership Conference. *April 2021.*
- Panelist, "From Prize Challenge, to Operations: Lessons from the xVIEW Challenge" and "Using AI to Understand Relationships Between People, Places, and Things: What are Knowledge Graphs and Why Should DoD Use Them Now?" NDIA National Security AI Conference and Exhibition (NSAICE) with DIU. *March 2021.*
- Panelist, "Smart commuting." Carnegie Mellon University Summit on U.S.-China Innovation and Entrepreneurship. *April 2021.*
- Panelist, "Ethics in AI." NASA AIML Expo: National AI Engineering Initiative. *July 2021.*

Carol Woody

- "Cybersecurity Engineering is Critical to Mission Success." Plenary presentation, 24th World Multi-Conference on Systemics, Cybernetics, and Informatics. *September 2020.*
- "DevSecOps Pipeline for Complex Software-Intensive Systems: Addressing Cybersecurity Challenges." Cyber Security and Information Systems Information Analysis Center (CSIAC) Webinar. *June 2021.*

Steven Wu

- "A Geometric View on Private Gradient-Based Optimization." Federated Learning One World Seminar. *March 2021.*
- "Involving Stakeholders in Building Fair ML Systems."
  - > Foundations of Algorithmic Fairness Workshop. *March 2021.*
  - > IDEAL Quarterly Theory Workshop: Algorithms and their Social Impact. *March 2021.*
  - > Trustworthy ML Initiatie (Trust ML) Seminar. *February 2021.*
- "Leveraging Heuristics in Private Synthetic Data Generation." The AAAI Workshop on Privacy-Preserving Artificial Intelligence. *October 2020.*

FEATURED **GRANTS RECEIVED BY FACULTY**

Alessandro Acquisti

- "The Impact of Ad-Blocking and Anti-Tracking on Consumers' Online Behavior and Welfare." *Funder:* The University of Pennsylvania Center for Technology, Innovation and Competition (CTIC) and the Warren Center for Network & Data. Other CMU researchers on the grant: Daphne Chang, Li Jiang.

Kathleen Carley

- "Culture in Power Transitions: Multi-Level Models of Covert Online Information Campaigns." *Funder:* Office of Naval Research.
- "MURI: Persuasion, Identity, & MOrality in Social-Cyber Environments." *Funder:* Office of Naval Research.
- "Cognizant Center of Excellence Content Moderation Research Program." *Funder:* Cognizant US Foundation.

Yuejie Chi

- "Learning to Prevail: Communication in Contested and Adversarial Environments." *Funder:* Air Force Research Laboratory.
- "CIF: Small: Resource-Efficient Statistical Inference in Networked Environments." *Funder:* National Science Foundation.

Lorrie Cranor and Lujo Bauer

- "Exploring Privacy Concerns and Solutions for AR Glasses." *Funder:* Facebook.

Lujo Bauer, Matt Fredrikson, Cleotilde Gonzalez

- "MURI: Cyber Autonomy through Robust Learning and Effective Human-Bot Teaming." *Funder:* Army Research Office.

Cleotilde Gonzalez

- "Advancing Learning Science for Improved Human-Machine Team Effectiveness." *Funder:* Air Force Research Laboratory, Sub-award from L3 Technologies, Inc., Link, Simulation & Training.

Hoda Heidari

- "Fairness in AI." *Funder:* National Science Foundation. Other CMU researchers on the grant: Rayid Ghani, Zachary Lipton, Alexandra Chouldechove, Kit Rodolfa.

Hanan Hibshi

- "picoCTF Student Diversity." *Funder:* Cisco.

Jason Hong

- "Harnessing Everyday Users' Collective Power to Audit Algorithmic Bias in AI Systems." *Funder:* Cisco. Other CMU researchers on the grant: Motahhare Eslami, Ken Holstein, Adam Perer, Nihah Shah, Hong Shen.
- "Peekaboo: Providing Architectural Support for Building Privacy-sensitive Smart Home Apps." *Funder:* Cisco. Other CyLab researchers on the grant: Yuvraj Agarwal, Swarun Kumar.
- "Organizing Crowd Audits to Detect Bias in Machine Learning." *Funder:* National Science Foundation. Other CMU researchers on the grant: Motahhare Eslami, Ken Holstein, Adam Perer, Nihar Shah, Hong Shen.
- "Helping People Manage Privacy Settings Using Social Influences." *Funder:* Facebook. Other CyLab researchers on the grant: Laura Dabbish.
- "Organizing Crowd Workers to Categorize Bias in ML Systems with Bias Bounties." *Funder:* Amazon. Other CMU researchers on the grant: Nina Balcan, Adam Perer, Hong Shen.

Lujo Bauer, Matt Fredrikson, Zico Kolter (shown right), Corina Pasareanu (shown below), P. Ravikumar

- "Provably Robust Deep Learning." *Funder:* DARPA

Swarun Kumar, Bob Iannucci (shown right), Anthony Rowe

- "Averting Wireless Spectrum Pollution in the Era of Low-Power IoT." *Funder:* NSF.
- "Harnessing Wireless Actuation." *Funder:* NSF.

Justine Sherry, James Hoe (shown right), Franz Franchetti (shown below), Vyas Sekar

- "Crossroads 3D-FPGA Academic Research Center." *Funder:* VMWare / Intel.

Steven Wu

- "Empowering and Enhancing Workers Through Building a Community-Centered Gig Economy." *Funder:* NSF Smart and Connected Communities Award. Other CMU researchers on the grant: Haiyi Zhu, David Burtch, Yanhua Li, Min Kyung, and Zhiwei Lee.

FEATURED **CYLAB RECOGNITIONS**

Kathleen Carley

- Served as the Conference Chair for the 2020 SBP-BRiMS International Conference.

Yuejie Chi

- Named the 2021 IEEE Information Theory Society Goldsmith Lecturer.

Lorrie Cranor

- Named a 2020 AAAS Fellow for contributions to usable privacy and security research, policy, and education.
- Received a CHI 2021 Best Paper Award Honorable Mention for her team's paper, "You Gotta Watch What You Say": Surveillance of Communication with Incarcerated People. Co-authors included Kentrell Owens and Camille Cobb.
- Received a 2020 Privacy Papers for Policy Makers Student Paper Honorable Mention for her team's paper, "It's a scavenger hunt": Usability for Websites' Opt-Out and Data Deletion Choices. Co-authors included Hana Habib, Sarah Pearman, Jiamin Wang, Yixin Zou, Alessandro Acquisti, Norman Sadeh, and Florian Schaub.

Matt Fredrikson

- Received "spotlight presentation" recognition at the International Conference on Learning Representations for Fast Geometric Projections for Local Robustness Certification with co-authors Aymeric Fromherz, Klas Leino, Bryan Parno, and Corina Pasareanu.
- Received a 2020 NSF CAREER Award.

David Garlan

- Received the SEAMS 2009 Most Influential (Test-of-Time) Award for the paper, Evaluating the Effectiveness of the Rainbow Self-Adaptive System. Co-authors included Shang-Wen Cheng and Bradley Schmerl.
- Received a Best Student Paper Award at SEAMS 2021 for their paper, Hey! Preparing Humans to do Tasks in Self-adaptive Systems. Co-authors included Nianyu Li, Javier Camara, Bradley Schmerl, and Zhi Jin.

Cleotilde Gonzalez

- Served as a committee member of the National Academy of Sciences (NAS) study on Enhancing Human-AI Teaming (Ehat). United States AirForce Research Laboratories.
- Named a Lifetime Fellow of the Cognitive Science Society.
- Served as a member-at-large of Division 3, Society for Experimental Psychology and Cognitive Science, of the American Psychological Association.
- Received the Best Paper Award at the 2020 International Conference on Decision and Game Theory for Security for their paper, Exploiting Bounded Rationality in Risk-based Cyber Camouflage Games. Co-authors include Omkar Thakoor, Shahin Jabbari, Palvi Aggarwal, Milind Tambe, and Phebe Vayanos.

Swarun Kumar

- Received the 2021 ACM SIGBED Early Career Researcher Award.
- Received a Best Paper Award at IPSN 2021 for the paper, Locating Everyday Objects using NFC Textiles. Co-authors included Jingxian Wang, Jumbo Zhang, Ke Li, Chengfeng Pan, and Carmel Majidi.
- Received a Best Wearables Long Paper Award at ACM UbiComp 2020 for their paper, RFID Tattoo: A Wireless Platform for Speech Recognition. Co-authors included Jingxiang Wang, Chengfeng Pan, Haojian Jin, Vaibhav Singh, Yash Jain, Jason Hong, and Carmel Majidi.
- Received a Best Paper Honorable Mention at ACM MobiSys 2020 for their paper, Osprey: A mmWave Approach to Tire Wear Sensing, with co-authors Akarsh Prabhakara, Vaibhav Singh, and Anthony Rowe.

Justine Sherry

- Received the VMWare Systems Award in recognition of her seminal contributions to the field of networking.

Carol Woody

- Inducted into IEEE-HKN (Eta Kappa Nu), the Academic and Professional Honorary Society recognizing excellence in the IEEE-designated fields of interest.

Steven Wu

- Best paper award at the Distributed and Private Machine Learning (DPML) and the Synthetic Data Generation workshop, both at ICLR 2021, for their paper, Leveraging Public Data for Practical Private Query Release, with co-authors Terrance Liu, Giuseppe Vietri, Thomas Steinke, and Jonathan Ullman.

Osman Yagan

- Received a 2020 IBM Faculty Award.
- Received a Best Paper Award with Mansi Sood at the 2021 IEEE International Symposium on Communications for their paper, Tight Bounds for the Probability of Connectivity in Random K-out Graphs.

The New York Times

10.22.2020 On working from home:

"First of all, turn off your camera when you don't need it. When your camera is on, make sure your computer is facing the wall."

Lorrie Cranor, *Director and Bosch Distinguished Professor in Security and Privacy Technologies, CyLab; FORE Systems Professor of Computer Science and of Engineering & Public Policy*

"We are all responsible for setting boundaries between our personal and professional lives. Behave as though you are physically in the office even when working from home."

Dena Haritos Tsamitis, *Director, Information Networking Institute; Barbara Lazarus Professor in Information Networking; Founding Director, Education, Training and Outreach, CyLab*

The Christian Science Monitor

11.3.2020 On misinformation:

"As opposed to just pointing out that something is wrong, provide an alternative."

Kathleen Carley, *Professor of Computation, Organizations, and Society, Institute for Software Research*

POPULAR SCIENCE

1.8.2021 On facial recognition:

"The main thing to realize is that facial recognition is not perfect. It comes up with a ranked order list of individuals."

Marios Savvides, *Bossa Nova Robotics Professor of Artificial Intelligence, Electrical and Computer Engineering*
Director, CyLab Biometrics Center

BUSINESS INSIDER

4.16.2021 On iPhone security:

"Install apps from trustworthy sources and unless you know what you're doing, you probably don't want to jailbreak your phone. Be careful. Don't click on attachments you don't want to open and keep your phone up to date."

Vyas Sekar, *Tan Family Professor of Electrical and Computer Engineering*

The Washington Post

4.26.2021 On Russian hacks:

"I don't think we're done seeing Biden's response to SolarWinds. SolarWinds is one of many incidents where Russia is using cyber, and Biden's administration is looking at them holistically as part of a total national security policy."

David Brumley,
Professor, Electrical and Computer Engineering

Bloomberg

5.6.2021 On broadband:

"Upstream is critical if you're working or taking classes from home. We found that after the pandemic hit, downstream speed stayed about the same but upstream speed was significantly degraded, and consumer complaints about speed tripled."

John Peha, *Professor, Engineering and Public Policy*

Authority Magazine

5.25.2021 On pursuing a cybersecurity career:

"There is room for every skill in cybersecurity. There is a certain stereotype about cybersecurity that is not true and I encourage everyone to educate themselves about the field."

Hanan Hibshi, *Assistant Teaching Professor, Information Networking Institute*

Newsweek

6.11.2021 On Bitcoin and the Colonial Pipeline hack:

"It just highlights that bitcoins are traceable, which has never been in doubt. This has nothing to do with the underlying technology."

Nicolas Christin,
Associate Professor, Engineering and Public Policy, Institute for Software Research

TIME

6.14.2021 On biometrics:

"Biometrics' range of potential uses is vast: from benign, such as secure access to the app—think about how [Apple's] iOS uses facial recognition for authentication—to chilling, such as mass re-identification and surveillance."

Alessandro Acquisti, *Professor of Information Technology and Public Policy at the Heinz College*

CYLAB **CORE FACULTY**

CyLab's faculty bring security and privacy expertise from across the University. In addition to our core faculty, we have over 80 affiliate faculty.

Alessandro Acquisti
Professor, Heinz College

Yuvraj Agarwal
Associate professor, Institute for Software Research (ISR)

Ehab Al-Shaer
Professor, ISR and Computer Science Department (CSD)

Lujo Bauer
Professor, Electrical and Computer Engineering (ECE), ISR

Shawn Blanton
Professor, ECE

David Brumley
Professor, ECE

Yang Cai
Senior systems scientist, CyLab, *Director*, Visual Intelligence Studio

Nicolas Christin
Associate professor, Engineering and Public Policy (EPP), ISR

Lorrie Cranor
Director and Bosch Distinguished Professor in Security and Privacy Technologies, CyLab, *FORE Systems professor*, ISR, EPP

Anupam Datta
Professor, ECE

Giulia Fanti
Assistant professor, ECE

Matt Fredrikson
Assistant professor, CSD, ISR

Virgil Gligor
Professor, ECE

Vipul Goyal
Associate professor, CSD

Dena Haritos Tsamitis
Director and Barbara Lazarus professor in Information Networking, Information Networking Institute (INI), *Founding director, education, training and outreach*, CyLab

Hanan Hibshi
Assistant Teaching Professor, INI

Jason Hong
Professor, Human-Computer Interaction Institute

Limin Jia
Associate research professor, ECE, INI

Aleecia McDonald
Assistant professor of the practice, INI

Bryan Parno
Associate professor, CSD, ECE

Corina Pasareanu
Principal systems scientist, CyLab

Raj Rajkumar
George Westinghouse professor, ECE

Norman Sadeh
Professor, ISR

Marios Savvides
Bossa Nova Robotics professor of artificial intelligence, ECE, *director*, CyLab Biometrics Center

Vyas Sekar
Professor, ECE

Elaine Shi
Associate professor, CSD, ECE

Asim Smailagic
Research professor, ECE

Patrick Tague
Associate research professor, INI

Conrad Tucker
Professor, Mechanical Engineering

Sam Weber
Senior Systems Scientist, CyLab

Maverick Woo
Systems scientist, CyLab

Osman Yagan
Associate research professor, ECE

Ding Zhao
Assistant professor, Mechanical Engineering, Robotics Institute

NEW CYLAB FACULTY

Wenting Zheng, an assistant professor in the Computer Science Department focused on computer systems, security, and applied cryptography, joined CMU this Fall.

THE CYLAB PARTNERS CONFERENCE **GOES VIRTUAL!**

Even the pandemic could not stop dozens of CyLab researchers from convening with industry practitioners, as the 2020 CyLab Partners Conference was held completely virtually. Attendees received special CyLab socks, and many were not shy about bragging about attending the conference...in their socks.

PARTNERS PASSIONATE ABOUT CREATING TRUST THROUGH TECHNOLOGY AND EDUCATION

Carnegie Mellon CyLab is a world leader in innovative thinking and game-changing collaborations that make life more safe, secure and privacy-respecting. We welcome industry and government agencies to join us in what we do best: solving real-life problems through interdisciplinary research and education. From building visibility among students to gaining access to cutting-edge faculty research, upskilling your workforce, and launching new initiatives for social good, CyLab partnership opportunities offer both immediate and far-reaching results.

CyLab's partners include a wide variety of businesses and institutions, ranging from companies focused on developing advanced technologies for the Internet of Things (IoT) to science and government agencies in the USA and international partner countries. These organizations have access to research and education opportunities that spur industry-wide advancement, propel employees' skills, and transform promising ideas into marketplace triumphs. Strategic focus initiatives include rethinking Future Enterprise Security through innovations in artificial intelligence, computer science, engineering, and human factors, and creating the knowledge and capabilities to build and implement Secure Blockchain systems "beyond-the-hype".

To work together to come up with a collaboration plan that benefits your team and CyLab, contact Michael Lisanti, Director of Partnerships at partnerships@cylab.cmu.edu.

CYLAB NEWS BRIEFS

All of these exciting news stories can be read in-full at cylab.cmu.edu/news.

AUG26

Ads may not provide benefits companies say they do

A recent study by researchers in CyLab and Heinz College tests claims by the advertising industry that online ads help consumers find better, cheaper products faster.

SEP21

Jin receives 2020 UbiComp Outstanding Student Award

Haojian Jin, a fifth year Ph.D. student, received the Gaetano Borriello Outstanding Student Award during the virtual UbiComp 2020 awards ceremony.

SEP28

picoCTF to hold 2020 Mini Competition in October

In celebration of National Cybersecurity Awareness Month, picoCTF will be holding a mini competition during the month of October. The competition will consist of series of cybersecurity challenges of intermediate difficulty in the topics of reverse engineering, forensics, web, and binary exploitation problems.

SEP30

Websites containing COVID info are tracking you

In a new study, CyLab's Tim Libert showed that 99 percent of websites that contained information regarding COVID-19 also contained code that shares user activity data with third parties, including advertisers.

OCT02

Recognizing AI's misinformation

What does cybersecurity have to do with human recognition of false data? A lot, says Conrad Tucker, who teamed up with Challenger Center and RAND to study the link between the two.

OCT08

Cyber defense is an art in human deception

CyLab's Coty Gonzalez and her research group presented two studies on cyber deception at the Human Factors and Ergonomics Society annual meeting. CyLab director Lorrie Cranor gave the meeting's keynote talk.

OCT15

Intelligent, automatic contact tracing

CMU ECE alumnus Patrick Lazik and his team at Yodel Labs have developed a system that creates contact networks to contain COVID-19.

OCT20

Finally: a usable and secure password policy backed by science

After nearly a decade of studies, the passwords research group in CyLab has developed a policy for creating passwords that maintains balance between security and usability—one backed by hard science.

OCT28

New tool simplifies data sharing, preserves privacy

According to a new study authored by researchers in CyLab and IBM, a new tool can help circumvent the privacy issue in data sharing.

OCT30

Four years since the Mirai-Dyn attack...is the Internet safer?

Four years after the Mirai-Dyn attack that brought down much of the Internet, a team of CyLab researchers are assessing the Internet's resilience if a similar attack were to occur today.

NOV05

World's fastest open-source intrusion detection is here

Researchers in CyLab have developed the fastest-ever open-source intrusion detection system—one that achieves speeds of 100 gigabits per second using a single server.

NOV20

CMU announces partnership with the Cybersecurity Manufacturing Innovation Institute

CyManII's vision is to introduce a cyber-secure energy-ROI for energy efficient manufacturing and supply chains that secures and sustains American leadership in global manufacturing competitiveness for decades.

NOV24

Lorrie Cranor named AAAS Fellow

Lorrie Cranor has been named a Fellow of the American Association for the Advancement of Science (AAAS for her contributions to usable privacy and security research, policy, and education.

DEC03

App and infrastructure alert users about data collection around them

The IoT Assistant app and digital infrastructure, developed by researchers in CyLab, paves the way for people to take control of their privacy amid the booming Internet of Things.

DEC11

CyLab researchers design privacy icon to be used by California law

The state of California has proposed an official icon to include next to opt-out text—a blue stylized toggle icon developed by researchers from CyLab and the University of Michigan's School of Information. Users may begin seeing the new stylized icon at the bottom of websites' footers early next year.

DEC16

Justine Sherry wins 2020 VMWare Systems Research Award

CyLab's Justine Sherry is the winner of the 2020 VMWare Systems Research Award, in recognition of her seminal contributions to the field of networking.

DEC18

IoT@CyLab sharpens focus on Industrial IoT

Carnegie Mellon's Secure and Private IoT initiative (IoT@CyLab has recognized the so-called Industrial IoT (IIoT as the next big challenge in IoT security.

JAN07

Gonzalez named 2021 Fellow of Cognitive Science Society

The Cognitive Science Society announced seven research scientists, including CyLab's Cleotilde Gonzalez, as 2021 Fellows. Gonzalez joins a selected group of 120 researchers, who have been recognized for their sustained excellence and impact on the cognitive science community.

JAN12

What if opting out of data collection were easy?

Recent work by researchers in CyLab has shown that it is possible to use machine learning techniques to automatically extract and classify some of these opt-out choices, and introduces a new, handy browser extension.

FEB19

Phishing, fairness, and more: CyLab's 2021 seed funding awardees

Over $350K in seed funding has been awarded to 14 different faculty and staff in seven different departments across three colleges at CMU.

MAR09

The world's largest online hacking competition launches next week

picoCTF 2021 begins March 16 at 12 p.m. and concludes March 30 at 3 p.m. ET. Participation is free, and all one needs to participate is a computer with basic Internet access.

MAR17

CMU and Pitt launch center dedicated to combating extremist hate

Carnegie Mellon University and the University of Pittsburgh jointly launched a new center to study extremist hate. Scholars at both universities will partner through the Collaboratory Against Hate—Research and Action Center to develop effective tools that inhibit hate's creation, growth, and destructive consequences.

MAR31

Corina Pasareanu receives ETAPS' Test of Time Award

Corina Pasareanu, a researcher in CyLab, has received a Test of Time Award from the European Joint Conferences on Theory and Practice of Software (ETAPS.

APR21

Former federal CISO Touhill named new director of CMU SEI CERT Division

Carnegie Mellon University's Software Engineering Institute today announced the appointment of Gregory J. Touhill as director of the SEI's CERT Division.

APR22

Carnegie Mellon CyLab partners with Rolls-Royce and Purdue

As the world continues its trend toward digitization, Carnegie Mellon University has announced the launch of a new research partnership with Rolls-Royce and Purdue University to focus on enhancing the security of embedded system platforms.

APR23

picoCTF announces 2021 competition winners

picoCTF, which over the course of nearly a decade has become the world's largest online hacking competition, held its 2021 competition.

MAY11

Study explores privacy of prison communications

The study, which explores people's understandings, attitudes, and reactions to prison surveillance, received an Honorable Mention award at this week's Association for Computing Machinery (ACM Computer-Human Interaction (CHI conference.

MAY13

CyLab researchers develop new guidance for designing privacy choices

In a new study presented at this week's ACM CHI conference, CyLab researchers outlined a set of standards and taxonomy to help alleviate the void in guidance that still leaves privacy choices muddied for users.

MAY26

CyLab's IoT security and privacy label effectively conveys risk, study finds

The study, presented at the IEEE Symposium on Security and Privacy, helps bridge the gap between experts' knowledge and consumers' understanding of privacy and security risks.

MAY28

CMU CyLab to co-host this year's PEPR Conference

This year's Privacy Engineering Practice and Respect (PEPR Conference will be co-hosted by CyLab and the Future of Privacy Forum, and will be held virtually June 10-11.

JUN07

CyLab researchers discover novel class of vehicle cyberattacks

The new class of vulnerabilities was disclosed in a new study presented at the IEEE Symposium on Security & Privacy, held virtually.

JUN10

Internet performance during COVID not as great as many say, study shows

Internet performance suffered substantially during the COVID-19 pandemic, according to a new study by researchers in Carnegie Mellon University published this week in the Journal of Information Policy.

JUN14

Interdisciplinary research for an intersectional student

Aurelia Augusta, co-advised by CyLab's Lorrie Cranor, works to improve online experiences.

JUN15

A big step towards cybersecurity's holy grail

The trek towards the holy grail of cybersecurity—a user-friendly computing environment where the guarantee of security is as strong as a mathematical proof—is making big strides.

JUN17

How to teach about privacy... using "potty talk"

Lorrie Cranor believes that bathrooms—these very intimate spaces for people of all ages—are surprisingly useful for conveying concepts related to both privacy and usability.

JUN18

CyLab researchers shine at PEPR 2021

More than 500 people gathered virtually at the PEPR conference, perhaps the largest gathering of privacy engineers ever.

JUL15

Misconceptions plague security and privacy tools

According to a new study out of CyLab, people hold a myriad of misconceptions about the security and privacy tools out there meant to help protect our privacy and online security.

JUL19

One size does not fit all when managing data practices on the web

A new study by Carnegie Mellon University CyLab researchers aimed to learn about users' awareness of data practices, how they felt about them, and how much control they perceived to have over them.

JUL22

Study explores tensions between IoT device owners and "incidental users"

A team of CyLab researchers conducted a study exploring the tensions that may arise between device owners and incidental users, who may or may not be comfortable as incidental users.

JUL29

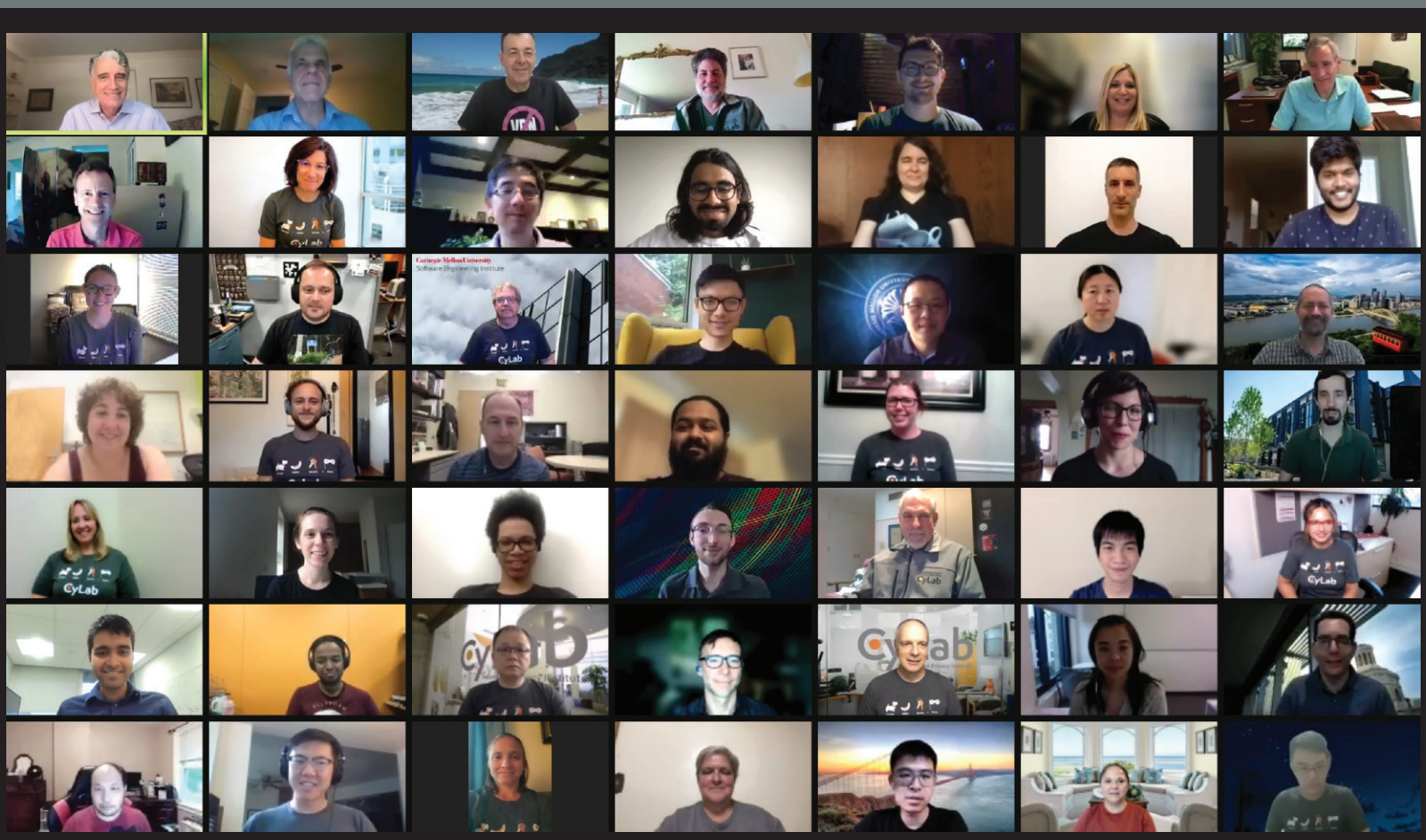
Two CyLab papers presented at the FTC's PrivacyCon 2021

The FTC selected fewer than 20 papers to be presented at this year's PrivacyCon, and two of them were written by CyLab researchers.

JUL30

Do you hear what I hear? A cyberattack.

In a new study presented this week at the Conference on Applied Human Factors and Ergonomics, Cai and two co-authors show how cybersecurity data can be heard in the form of music.



Carnegie Mellon University
Security and Privacy Institute
CyLab