# 2019–2020 CYLAB YEAR IN REVIEW


Carnegie Mellon University
CyLab
Security and Privacy Institute

# Letter from the director

## DEAR FRIENDS

This year's CyLab Year in Review focuses on some of the ways CyLab is having an impact on the world. I'm proud that our faculty and students are winning awards for their research (note especially five CyLab research papers winning IEEE Security & Privacy Test of Time awards!), but I'm especially enthusiastic about the real world impact that CyLab researchers are having.

In this issue we focus on impacts related to the current pandemic. In particular, we explore the work Kathleen Carley has been doing tracking disinformation related to COVID-19 and Jason Hong's research on privacy and contact tracing apps. When the pandemic reached the US, Yang Cai leveraged his recent research that resulted in an award-winning smart helmet for firefighters to quickly pivot and develop remote fever scanning technologies for first responders.

CyLab research also continues to have real-world impact unrelated to the current pandemic. This spring research submitted by CyLab researchers to the California Attorney General's office on the use of "Do Not Sell My Personal Information" icons on websites influenced California's decision not to introduce a confusing icon. In April, code from Bryan Parno's correct and secure "EverCrypt" cryptographic library was officially incorporated into the Linux kernel. Three CyLab papers were selected for presentation at the US Federal Trade Commission's annual PrivacyCon event, which is designed to educate policymakers about the latest research and trends in consumer privacy and data security. And I was excited to see Apple announce in June that they will introduce privacy "nutrition labels" for mobile apps, a concept we started researching over a decade ago in CyLab.

CyLab researchers are known not only for our strong technical work in security and privacy, but also for our interdisciplinary work, which is driven by collaborations across the entire university. From the beginning, CyLab research has been published not only in computer science conferences, but also in social science, public policy, and law journals. In the past year we pushed our interdisciplinary boundaries even further as CyLab researchers collaborated on not one, but two, new theater productions focussed on privacy and AI. Those of you who attended our 2019 Partners Conference had the opportunity to experience *Project Amelia* first hand and meet the playwright (and CyLab faculty member) Michael Skirpan.

I'm also proud of the way CyLab students, faculty, and staff have come together while being physically apart during the pandemic. Despite many challenges, the work of CyLab has continued remotely. Besides the stress of living through a pandemic, many of our colleagues struggled with working from home without outside childcare. We adjusted to the new normal, helped each other out, and welcomed children, dogs, and even ducks to our regular Zoom meetings.

After George Floyd was murdered by police in May, members of the CyLab community joined people around the world in protesting and demanding change. In CyLab we held virtual community discussions and developed a list of action items that we have already started working on to promote a culture of inclusiveness and equity in CyLab that is intolerant of racism, discrimination, and bias. We are finding ways to integrate discussions of racism and systemic injustice into our CyLab research, educational, and community-building efforts, and we are committed to recruiting and helping to develop more students, faculty, and staff who are Black or members of other underrepresented groups.

As we head into the Fall semester we expect that many of our activities in CyLab will remain remote for at least the next several months. Nonetheless, the work of CyLab continues. We are welcoming new students and faculty (including Elaine Shi, a CyLab alumna from 2008 who has just joined our faculty and is the winner of our first annual CyLab Distinguished Alumni Award), teaching classes, conducting research, writing papers, presenting them (virtually) at conferences, and continuing to make an impact on the world.

Lorrie Cranor

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

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

# CyLab responds to COVID-19

## CyLab faculty have been focusing their work on security and privacy impacts of the coronavirus pandemic.

A lot has changed in the world in 2020. The COVID-19 pandemic uprooted our daily lives, transforming many of our homes into our workplaces. The pandemic has touched many aspects of security and privacy, and CyLab researchers have been quick to jump in and contribute their expertise in solving some of the biggest security and privacy issues that have arisen this year.

## Tracking the spread of disinformation during the pandemic

*CyLab's Kathleen Carley has been closely monitoring the spread of disinformation related to the coronavirus pandemic.*

Amid the global coronavirus pandemic, disinformation about the situation has been spreading at lightning speeds on social media. In the words of Kathleen Carley, a CyLab faculty member and a professor in the School of Computer Science's Institute for Software Research, "This is dangerous." Her research group has been closely monitoring the situation and sharing their findings on a regular basis.

During her academic career, Carley has studied disinformation campaigns around all kinds of events, ranging from elections to natural disasters. But what she's observed during this pandemic is quite different.

In a preliminary study conducted in March, her research group found that roughly 40 percent of the discussion around coronavirus and COVID-19 was coming from social media bots. Of the users themselves engaging in conversation about the virus, her group found that 22 percent of them were bots.

"A big issue is that these bots are very influential—the network around them is configured such that they have a lot of listeners," says Carley.

Her study found that 42 percent of the top 50 influential mentioners were bots, 82 percent of the top 50 influential re-tweeters were bots, and 62 percent of the top 1,000 re-tweeters were bots.

"This means that, similar to the virus itself, disinformation about the virus is spreading quickly – only much, much faster."

Compared with elections, Carley says that there is a lot more disinformation related to the coronavirus, and the disinformation is less personalized. For example, a large fraction of the disinformation suggests fake cures and fake prevention. Compared with natural disasters, the disinformation isn't terribly different; she's observing similar stories about fake emergency measures.

"For example, some disinformation was being spread at one point that New York City was locked down under martial law," Carley says. "That was and is not true."

On an uplifting note, Carley says that social media companies are stepping in to help.

"Unlike the situation during previous elections, a lot of social media companies are trying to combat disinformation around coronavirus right now," she says.

Carley's advice for social media users isn't very different from previous advice she has offered: call out disinformation that you see, and don't share satire or jokes about COVID-19 because not everyone will understand that it is satire.

"During elections, sharing disinformation poses a threat to democracy. That is very bad," Carley says. "But in this situation, if you follow the guidelines in some of the disinformation, you could actually harm yourself."

Carley's ongoing research is being conducted in the Center for Informed Democracy and Social Cybersecurity (IDeaS) and the Center for Computational Analysis and Organizational Systems (CASOS) at Carnegie Mellon University.

# Privacy perceptions of contact-tracing apps

Contact-tracing could help curb the spread of COVID-19. While the process can be performed manually, researchers have suggested that digital contact tracing using cell phones could be a more accurate and scalable approach. But its effectiveness relies heavily on a large installation rate—and that may depend on how people weigh the app's utility versus its privacy risks.

Researchers at Carnegie Mellon University examined user preferences on six different app designs after explaining the risks and benefits of each option—including whether the user's data was stored on a centralized (government) server or decentralized server run by the app's developer.

"Surprisingly, contrary to the assumptions of some previous work, we found that the majority of people in our sample preferred to install apps that use a centralized server for contact tracing," said Tianshi Li, a doctoral student advised by CyLab's Jason Hong in the School of Computer Science's Human-Computer Interaction Institute (HCII).

Contact-tracing apps may need to collect a lot of sensitive health and personal information, including where you've been, who you've been interacting with and if you've been diagnosed.

"The problem is that decentralized solutions are not risk free," Li said. "We found that people are more willing to allow centralized authorities to access information than to allow a decentralized server to potentially offer loopholes to tech-savvy users who could infer the identity of diagnosed users."

The largest cluster of people, 32 percent of the sample, preferred centralized versus decentralized servers. The second largest cluster, 25 percent, were the most privacy-conscious and disagreed with almost all app designs.

Another design aspect included in the survey is location data sharing. Researchers found that a majority of the sample preferred to install apps that share diagnosed users' recent locations in public places to show infection hotspots. "People are generally very sensitive about location data, but in this specific case, users wanted useful information, beyond even direct exposure notice, so they feel more in control of the situation and can make their own decisions about how to reduce risk," Li said.

The researchers offer several suggestions for an app design that may achieve a high adoption rate in the U.S.

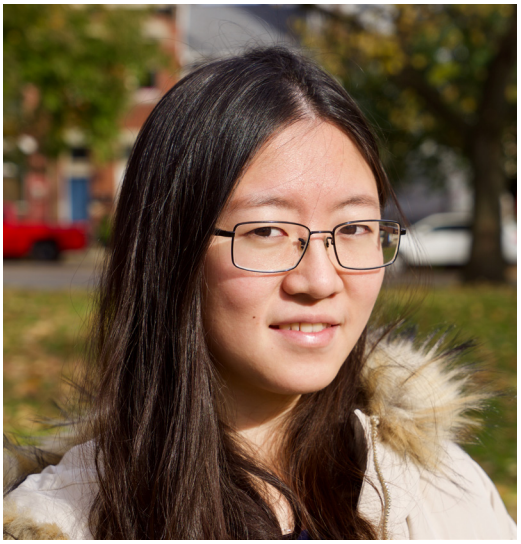
First, servers should be centralized, although Li underscored the importance of handling data in a secure and privacy-preserving manner, and verifying the users' identities during sign up to avoid malicious users identifying diagnosed users. Also, a one-size-fits-all solution has its challenges. Researchers found that at the state level, political leaning influenced design preference. Li said a combination of manual and digital contact tracing may be necessary.

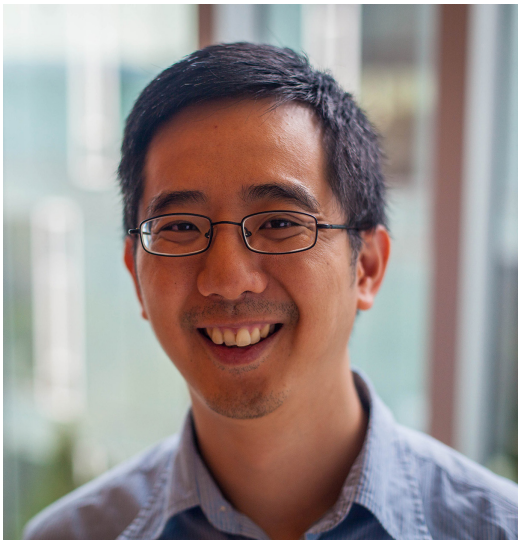
The researchers' second suggestion is to provide users with information about infection hotspots, which may nudge them to install the app. Location data collection should be opt-in, and the app should offer multilevel options when it requests that data to accommodate different user preferences.

Finally, researchers said these apps should be transparent about the risks of disclosing personal information to both governments and tech-savvy users.

"I think this is the very first step to understand the design space," Li said. "Challenges are obvious, such as keeping a centralized server secure from hackers. But now is the time to think about design, before investments are made and apps make their way onto people's phones."

Currently, Apple and Google are only offering APIs for decentralized contact-tracing apps. Researchers believe that similar APIs may also be needed to support the implementation of centralized contact-tracing apps that follow the best security and privacy practices.





*Tianshi Li (left) and Jason Hong (right).*

# Remote fever-scanning technologies

As COVID-19 engulfs the world, businesses are looking ahead and preparing for their reopening. Responding to industry inquiries, Yang Cai is leading a team that's developing automatic remote fever-screening technologies that can make it possible for buildings and first responders to detect fevers from a distance.

Cai, a senior systems scientist in Carnegie Mellon University's CyLab and the director of the Visual Intelligence Studio, is working with research engineers Sean Hackett and Florian Alber to scan people's foreheads to detect fevers. The goal is to provide reopening businesses an affordable tool for screening people who enter their premises.

The challenge with the project lies in the complexity of human behaviors. People wear masks, bandanas, and hats, carry coffee mugs, walk in different directions, assume various poses, and these things make it difficult to detect someone's forehead.

Working in their home labs, the researchers developed an algorithm that can detect multiple faces and measure temperature on the forehead. They applied sensor fusion of multiple data sources to achieve the desirable accuracy for temperature screening. With their innovative fusion algorithm, the team was able to significantly reduce the false negative and false positive detection results. The system can perform self-calibration on the measurements with the factors of distance and ambient temperature. Compared to today's commercial thermal scanners, the researchers are building a system that delivers accuracy at lower costs.

Prior to this project, the team designed an award-winning smart helmet for firefighters, and they are drawing from this experience to transfer their work from the standalone fever-scanning system to one that is mounted on a helmet for mobile use. The technology is lightweight by design, and they built a prototype that features a battery-powered single board computer and a thermal imaging chip. The system's accuracy is dependent on the thermal chip, and the researchers are addressing inherent challenges with these kinds of chips.

*CyLab research engineer Florian Alber shows his group's fever-screening helmet.*

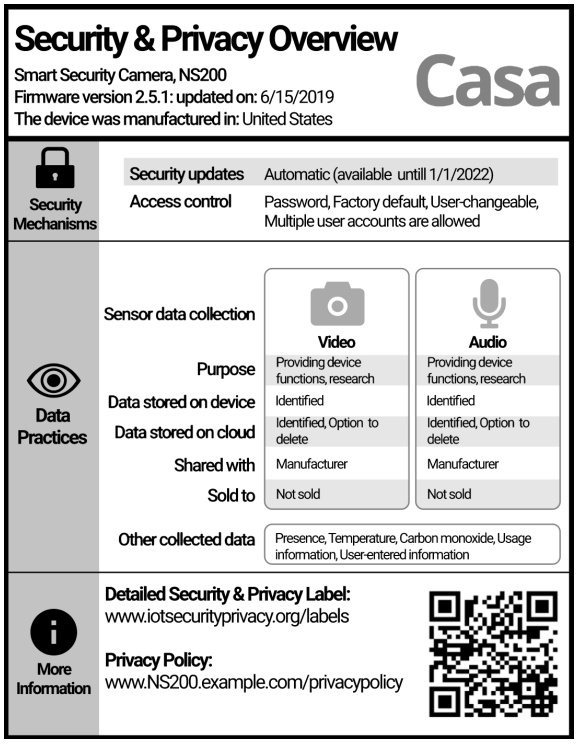
Despite the lockdown situation, the researchers were able to build the first prototype in merely nine days with available parts they had in their homes. They also performed preliminary testing and made improvements in the following weeks. The team intends to conduct further testing in buildings once the shutdown situation changes.

"This work demonstrates how resilient a research group can be with professional skills, cyber-collaboration tools like Zoom, Amazon deliveries, and commonly available parts. The lab has in fact operated more productively than before, without physical distractions and daily commuting," said Cai.

Although this is early-stage research, the team says the technology could be mounted above doorways to screen workers entering offices. The tool could add additional layers of security for a reasonable cost. The heads-up display on the helmet could be used by first responders to assess the situation of patients on the field.

The team has reached out to local museums and EMS teams about the technology and have launched the "Engineers Respond to COVID-19" Technical Lecture Series with IEEE Pittsburgh Section. Recently they have given talks on remote fever screening, haptic interfaces, and local data tracking and modeling.

# IoT labels will help consumers figure out which devices are spying on them




When hungry consumers want to know how many calories are in a bag of chips, they can check the nutrition label on the bag. When those same consumers want to check the security and privacy practices of a new IoT device, they aren't able to find even the most basic facts.

Not yet, at least.

In a study published in the proceedings of the IEEE Symposium on Security & Privacy, a team of researchers in Carnegie Mellon University's CyLab have developed a prototype security and privacy "nutrition label" that performed well in user tests. To develop the label, the team consulted with a diverse group of 22 security and privacy experts across industry, government, and academia.

The team also developed an IoT label generator for manufacturers to use to easily create labels for their devices.

"Survey results show that the vast majority of people are concerned about the security and privacy practices of devices, so we need to provide them with this information," says CyLab's Pardis Emami-Naeini, the study's lead author and a recent Ph.D. recipient in Societal Computing in the School of Computer Science. "The display of this information should be concise and understandable, akin to a nutrition label on food products."

A recent survey conducted by the Economist Intelligence Unit found that 89 percent of participants are uncomfortable with their personal data being shared with third parties without consent. Ninety-two percent of participants said they think it is important to inform consumers when personal data is being collected.

"Despite these concerns, people cannot find information about the privacy and security practices of devices at the moment of purchase," says Emami-Naeini.

The team's label consists of a primary layer meant to be displayed on the outside of a device's box, which conveys the most important information such as the type(s) of data the device collects, for what purpose, and with whom the data is shared. By scanning a QR code on the primary layer, consumers have access to a secondary layer of the label online that contains additional information such as how long the device retains data, and how often it is shared. Combined, both layers display 47 different pieces of information about a device's security and privacy practices.

Serving as a backdrop to the development of an IoT label, privacy regulations are calling for more transparency in how consumer data is collected and used. The Cyber Shield Act hopes to create a set of standards for IoT devices and then give labels to products that meet those standards. Similar efforts are moving forward internationally in the United Kingdom, Finland, and Singapore.

The team is currently in discussions with IoT device manufacturers and retailers, looking for companies interested in being early adopters of the label. Their goal is for their label to become an industry standard so that consumers would be able to readily learn about privacy and security features of their IoT devices and compare these features across devices, just as consumers compare calories and cholesterol in different food products.

The researchers are currently honing in on one particular finding in their study: that consumers are willing to pay a premium for devices that have a label like the one they developed.

"We want to conduct a realistic study to determine exactly how much consumers are willing to pay, as this would incentivize companies to adopt the label and be more transparent," says Emami-Naeini.

Other authors on the study included Associate Professor of Computer Science Yuvraj Agarwal, Information Networking Institute Research and Teaching Scientist Hanan Hibshi, and CyLab director Lorrie Cranor. Emami-Naeini was co-advised by Agarwal and Cranor.

# Five CMU security and privacy papers awarded IEEE's Test of Time award

Having a paper accepted to a high-caliber conference is a great accomplishment. Having one of those papers withstand the test of time is even better.

Five papers co-authored by Carnegie Mellon researchers presented at past IEEE Security & Privacy (S&P) symposia more than fifteen years ago were awarded IEEE's *Test-of-Time Award* at this year's annual conference. Papers written between 1995 and 2006 were eligible for this year's award, and a total of nine papers received the award.

"We looked for papers that initiated major new research directions and led to work – or even new research fields – that otherwise would not have emerged," said David Evans, Chair of the IEEE S&P Test of Time Awards Committee, at the IEEE S&P Test of Time awards ceremony.

In the paper presented at IEEE S&P 2005 titled, "Distributed Detection of Node Replication Attacks in Sensor Networks," authors Bryan Parno (CyLab), Adrian Perrig (CyLab), and Virgil Gligor (University of Maryland at the time, CyLab now) observed that in some networks, an attacker can capture a legitimate network node, extract its secrets, and then introduce many clones of that node back into the network. This gives the attacker significant influence over the network, allowing it to, for example, suppress legitimate alarms or subvert additional nodes.

To counter this threat, the study introduces a pair of protocols designed to detect replication via "emergent algorithms," which produce a network-level property via the independent actions of many nodes. This adversary model and problem formulation captured the community's interest, and led to some remarkable follow on work, both in sensor networks, and in other contexts, e.g., detecting fake accounts in social networks.

"We were proud of our work at the time, but we never expected it to have so much impact," Parno said during the IEEE S&P Test of Time awards ceremony.


In a paper presented at IEEE S&P 2003 titled, "Random Key Predistribution Schemes for Sensor Networks," authors Haowen Chan (CyLab), Adrian Perrig (CyLab, and Dawn Song (CyLab) helped advance security of communications between devices in the Internet of Things (IoT. Building off a paper from 2002, this paper extended the Eschenauer-Gligor model – by which sensors communicate using cryptographic keys – and identified three different ways to extend the resilience of the communication scheme.

"Community interest arose from the study as researchers started to embark and propose a series of ever-improved systems," Perrig said.

In a paper presented at IEEE S&P 2000 titled, "Efficient Authentication and Signing of Multicast Streams over Lossy Channels," authors Adrian Perrig (CMU), Ran Canetti (Boston University), Dawn Song, and J.D. Tygar (UC Berkeley; formerly CMU) introduce TESLA, a system for authentication of broadcast messages, also referred to as multicast streams. In order for secure broadcast authentication to be authenticated, only the sender can create the authentication information, and all the receivers can verify – but not create – the authentication. This "asymmetry" is difficult to achieve in an efficient manner. TESLA used time to achieve asymmetry, where a message is authenticated with a secret key that will be made public at a later point in time.

"We're extremely grateful and honored for receiving this award," Perrig said during the IEEE S&P Test of Time awards ceremony. "Over the past 20 years, the TESLA authentication system was used in a variety of real-world applications. Today, TESLA is being considered for the authentication of satellite navigation messages."

In another paper presented at IEEE S&P 2000, titled, "Practical Techniques for Searches on Encrypted Data," authors Dawn Song (UC Berkeley, formerly CMU, David Wagner (UC Berkeley), and Adrian Perrig (CMU) presented the first efficient construction to enable an untrusted server to perform a search on encrypted data without leaking the search term.

With the emergence of cloud computing, the paper inspired a wealth of follow-up research to further improve search operations, but also to support a variety of operations on encrypted data. With these systems, a user can perform operations on encrypted data in the cloud, without needing to trust the cloud operator.

"The paper was first published 21 years ago. The problem setting predates the rise of cloud computing by more than a decade," Song said at the IEEE S&P Test of Time awards ceremony.

Finally, in a paper presented at IEEE S&P 1996 titled, "A Sense of Self for Unix Processes," authors Thomas A. Longstaff (CMU SEI), Stephanie Forrest (Univ. of New Mexico, Steven A. Hofmeyr (Univ. of New Mexico, and Anil Somayaji (Univ. of New Mexico introduced a new method for network anomaly and intrusion detection in which "normal" is defined by short-range correlations in a process' system calls. The authors performed experiments that suggest that their "normal" definition is stable during normal behavior for standard UNIX programs.

The work was part of a research program aimed at building computer security systems that incorporate mechanisms and algorithms used by natural immune systems.

# Second round of Secure and Private IoT Initiative funded projects announced

Carnegie Mellon CyLab's Secure and Private IoT Initiative (IoT@CyLab) announced its second round of funding, which will support ten IoT-related projects for one year. While all Internet of Things security and privacy topics are within scope, IoT@CyLab is especially targeting the practical systems solutions for security of industrial control systems and Industrial IoT.

Funding for these projects was made possible by sponsorships from Amazon Web Services, AT&T Business, 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.

"With the increasing interest in industrial automation and trends toward 'Industry 4.0' it is critical that we develop a suite of solutions to secure these infrastructures and inform this critical transition," Rowe and Sekar shared in a joint statement. "We have an exciting array of research projects for year two spanning both novel hardware solutions, new ways of reasoning about cyber and cyber physical threats, as well as new applications of machine learning techniques in this setting."

The projects are grouped into three broad research themes: (1) Trustworthy platforms (2) Autonomous Healing Networks and (3) Accountability. In addition to these three research themes, we are also excited to add a new educational component, building on the success of CyLab's picoCTF platform to create custom modules for Industrial IoT Security.

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.

Listed below are the funded projects with each project's principal investigator(s) (PI).

### TRUSTWORTHY PLATFORMS

- **Hardware Redaction via Designer-Directed Fine-Grained eFPGA Insertion**
  PI: Ken Mai, Principal Systems Scientist, Electrical and Computer Engineering (ECE)
- **Lightweight Security Architectures for IoT Fog Networks**
  Co-PI: Osman Yagan, Associate Research Professor, ECE
  Co-PI: Swarun Kumar, Assistant Professor, ECE
- **Quantized Deep Neural Networks for Fingerprint Recognition**
  PI: Shawn Blanton, Trustee Professor, ECE

### ACCOUNTABILITY

- **Third-party Network Traffic Attribution for IoT, TV, Web, and Mobile**
  PI: Tim Libert, Special Faculty Instructor, ISR
- **IoTSniffer: Detecting Unauthorized Traffic in Industrial IoT**
  PI: Swarun Kumar, Assistant Professor, ECE
- **Privacy Tradeoffs in Distributed Learning**
  PI: Carlee Joe-Wong, Assistant Professor, ECE

### AUTONOMOUS HEALING NETWORKS

- **Systematic Attack Generation for Industrial Control Systems**
  PI: Eunsuk Kang, Assistant Professor, Institute for Software Research (ISR)
- **Robust Machine Learning-based anomaly detection for Industrial IoT**
  PI: Lujo Bauer, Professor, ECE and ISR
- **Zero-Knowledge Network Security Analysis using Generative Adversarial Networks**
  PI: Giulia Fanti, Assistant Professor, ECE

### EDUCATION

- **Expanding picoCTF into Industrial IoT**
  Co-PI: Hanan Hibshi, Research and Teaching Scientist, Information Networking Institute (INI)
  Co-PI: Maverick Woo, Systems Scientist, CyLab

For information on how your company can get involved in IoT@CyLab or other security and privacy research at CMU, contact Michael Lisanti, CyLab's director of Partnerships, at mlisanti@andrew.cmu.edu.

# CyLab researchers find Google's new congestion control algorithm does not treat data fairly

If the Internet had its own superhero, it might be the congestion control algorithm (CCA). CCAs are an essential piece of code Internet giants use to ensure that the Internet doesn't cripple amid a massive data traffic jam. They've been used since the 1980s to slow data transfers when they sense that a network is becoming overloaded.

Like any great superhero, CCAs try to work fairly; when the network is becoming overloaded, they won't prioritize one company's services over another.

However, research out of CyLab shows that a new CCA called BBR, developed by Google, can be unfair competing with other services in overloaded networks. Those findings were presented last Fall at the Internet Measurement Conference in Amsterdam.

"In a given network, our model shows that BBR would take up 40 percent of the bandwidth, leaving the remaining 60 percent to be split between the rest of the parties on the network," says Justine Sherry, a CyLab faculty member and an assistant professor in the Computer Science Department (CSD) at Carnegie Mellon University. "This goes against the concept of Internet fairness."


*Computer Science Ph.D. student Ranysha Ware presents her findings at the Internet Measurement Conference in Amsterdam.*

What does this mean for users? Imagine your home uses a 50 megabit per second (Mbps) connection provided by an Internet service provider. Most CCAs try to split the bandwidth evenly when many users want to use the network. If two users are each connected to a different Internet service, the CCA should try to give 25 Mbps to one user and 25 Mbps to the other.

CSD Ph.D. student Ranysha Ware, who led the research project on Internet fairness, was surprised when she ran experiments modeling network links and saw BBR exhibit very different behavior.

"When only two users are sharing the network, BBR's share is more than fair at 40 percent," Ware says. "But, as we added more users to the network, BBR did not give up any bandwidth as more users joined the network; it kept using 40 percent."

Imagine six people want to share the same 50 Mbps connection. A user connected to a service using BBR would get 20 Mbps of bandwidth, leaving the remaining 30 Mbps to be split between the other five users. Each user would get only 5 Mbps to work with. For video, this difference in bandwidth could be the difference between ultra-high definition video and standard definition.

In 2017, when Google first announced their algorithm, they claimed its design was fundamentally different from most current CCAs.

"People told us that it would be too hard to say anything mathematically provable about BBR because it works differently from traditional CCAs," says Sherry. But her team found that, indeed, BBR could be compared with other existing CCAs in terms of how it treats data using a mathematical approach based on congestion control windowing.

Is BBR going to harm Internet performance for its competitors?

"Only in the most congested links," Sherry says. "At my house, I have a 1 Gbps connection and it would be very hard to generate the kind of congestion that would make BBR hurt its competitors."

"BBR is a new and evolving algorithm," Sherry says. "We believe that BBR will probably change because of these findings."

# CyLab takes the stage

## CyLab faculty debut theater productions exploring AI and privacy

## *Project Amelia* provides a visit to the not-so-distant future

Michael Skirpan is very worried about the direction artificial intelligence (AI) is moving.

"We're taking judgments that humans make, where we take liability and responsibility of those judgments, and we're offloading them onto statistical models," says Skirpan, special faculty in Carnegie Mellon's Department of Philosophy. "Our moral decision-making and our social fabric are being moved into this technical algorithmic realm, which really has no moral compass to it. We're leaving it to the whim of pure business optimizations."

Skirpan's concerns manifested in the form of a screenplay he wrote a few years ago, which would eventually become a full-fledged immersive theater experience titled, *Project Amelia*. The play put attendees on the set of an R&D lab of a fictional tech giant. Attendees and actors on the set interacted with each other as the company prepared to launch a groundbreaking AI product.

Over the course of the play, major ethical concerns about the product arose, prompting actors and attendees to work together to try to see what's really going on under the company's hood.

"I thought it would be interesting if people were able to experience a piece of the future and be able to interrogate it first-hand and collectively with other people," Skirpan says.

*Project Amelia* ran its productions in Pittsburgh's South Side neighborhood in Fall 2019. Tickets were highly sought out, with most shows selling out weeks ahead of time. The production received rave reviews; here are a few of them.

The show was put on by Pittsburgh-based Bricolage Production Co. in collaboration with Probable Models, a consulting company with the tagline, "Making ethical futures more probable."

Also involved in the production: a cast of CyLab and other Carnegie Mellon researchers.

- **Lorrie Cranor**, director of CyLab | Research team
- **Maggie Oates**, Societal Computing Ph.D. student | Research team
- **Rob Cunningham**, Software Engineering Institute | Research team
- **Daragh Byrne**, School of Architecture | Research team
- **Eddy Man Kim**, School of Architecture | Architecture consultant
- **Eunsu Kang**, School of Computer Science | Interactive Media Curator
- **Carey Xu**, School of Drama | Architecture assistant

# *Looking at You* illustrates today's privacy dilemma in the form of an opera


In a world full of people staring at screens, Rob Handel believes that theatre is one of our last sacred spaces.

"Theatre is basically like church: you go into a room with a bunch of other people to have an experience, to which, in theory, you give your time and all of your attention," says Handel, a professor in Carnegie Mellon's School of Drama.

Handel is a librettist – a writer of operas. He's also very concerned about today's state of digital privacy. His most recent work, *Looking at You*, ran in New York City in Fall 2019 and explored issues of digital privacy in today's screen-filled world. The opera featured six singers, four musicians, and a conductor, and it dubbed itself as a "story of high-tech espionage and romance fusing Edward Snowden and Casablanca."

The opera received rave reviews from outlets like the Wall Street Journal and the New York Classical Review.

Handel tapped CyLab's Alessandro Acquisti for help in conveying the essence of digital privacy in his production.

Handel first heard Acquisti's name after he and Ralph Gross, a CMU School of Computer Science alumnus, published a study demonstrating that a person's social security number could be guessed with high accuracy with a mere photo on the Internet of that person. That finding, Handel says, really makes a person think twice about their daily interactions with the Internet.

"We wanted to find a way to bring these ideas to life on stage," says Acquisti, a professor of information systems in Carnegie Mellon's Heinz College. "The show integrates personal information about audience members into the story itself."

Acquisti's and Gross' main role with the production was creating the data mining infrastructure used to bring audience member's data into the show. During the show, attendees interact with tablets at their table on which they can choose whether or not to give the production team access to certain online information, such as their social media feeds.

The use of patron data, Handel says, tends to make the patrons who originally shared that data cringe.

"Imagine you're sitting in an opera, and a picture of your kid, who's at home with a babysitter, appears on a giant screen for the whole audience to see," Handel says. "We haven't stolen that picture from you – you put in on social media where anyone can see it. But now that picture is being shown to a room that you're sharing with 90 other people. You'd freak out."

Those 90 other opera attendees, Handel argues, probably have more in common with you than the people on the Internet as a whole. But you're still left uncomfortable.

"The Internet has made us disconnected from our understanding of what it means to be part of a society," Handel says.

After the show, attendees received a privacy kit put together by Acquisti that offered tips for better protecting and thinking more about sharing information online.

"One of my personal goals in participating in this work was to create awareness," says Acquisti.

Given *Looking at You*'s successful run in New York, Handel is hopeful that the show will go on tour sometime in the next year or two, as he says it was originally designed to do. As the show moves forward, one challenge that Handel and the rest of the production team will continue to face is the speed at which technology evolves.

"Theatre is a slow-moving artform. This took us years to develop, but technology changed a lot during that time," Handel says. "Obviously technology is really important right now, but it's hard to write anything about it because it moves faster than it plays."

# Over 39,000 people participated in this year's picoCTF hacking competition

*Students at Renton Prep Christian School in Renton, WA collaborate to solve a forensics challenge in picoCTF 2019.*

**The next picoCTF will be held March 16-30, 2021!**

**https://picoCTF.com**

**COMING SOON TO PICOCTF...**

- Non-competitive "gym"-like digital environment where people can learn and practice cybersecurity skills that will help prepare for competition
- Additional educational videos
- An online cybersecurity textbook for beginners

The biggest hacking competition keeps getting bigger.

Last Fall, over 39,000 people from all 50 US states and 160 different countries participated in picoCTF, a free online hacking competition hosted by Carnegie Mellon University. It was the fifth iteration of the competition since its original launch in 2013.

"My students learned more in a week than in the previous six weeks of class," said one teacher who had dozens of students participate from Albert G. Thomson High School in Georgia.

During the competition, which ran from September 27 - October 11, participants were tasked with solving up to 121 cybersecurity challenges 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.

The challenges themselves were housed in a retro-style video game with a unique storyline. Solving particular challenges unlocked other parts of the game's virtual world.

Cash prizes were awarded to the top five US-based middle and high school teams.

"While we offer prizes to middle and high school students, the challenges themselves are not 'dumbed-down' to middle school level," says Hanan Hibshi, research and teaching scientist in the Information Networking Institute and a faculty advisor behind picoCTF. "This year we saw a larger participation from university teams around the globe. picoCTF is for everyone who wants to learn about cybersecurity hands-on."

In a post-competition survey, two-thirds of participants claimed that they were "more interested" in pursuing a career in cybersecurity as a result of playing picoCTF 2019.

"It was an incredible experience for my students," said Josh Gold, a teacher at Nashoba Valley Technical High School in Westford, Mass. "I will be using PicoCTF with all of my 9-12 graders for as long as it exists."

picoCTF will hold its next official competition March 16-30, 2021.

In Fall 2020, the picoCTF development team will launch a series of new features, including a non-competitive "gym"-like digital environment where people can learn and practice cybersecurity skills that will help them during the competition. The new features, which also include educational resources, videos, and an online cybersecurity textbook for beginners, aim to provide year-round opportunities for learning cybersecurity skills beyond practicing in previous competitions.

**1st place: redpwn - 34,201 points**

- Tigard High School, Tigard, OR
- Whitefish Bay High School, Milwaukee, WI
- Kimberly High School, Kimberly, WI
- Interlake High School, Bellevue, WA

**2nd place: Flannel Forum of Forensics - 34,201 points**

- Montgomery Blair High School, Silver Spring, MD (2 members)
- West Windsor-Plainsboro High School North, Plainsboro Township, NJ (2 members)
- Suncoast High School, Riviera Beach, FL

**3rd place: GS Goofballs - 34,201 points**

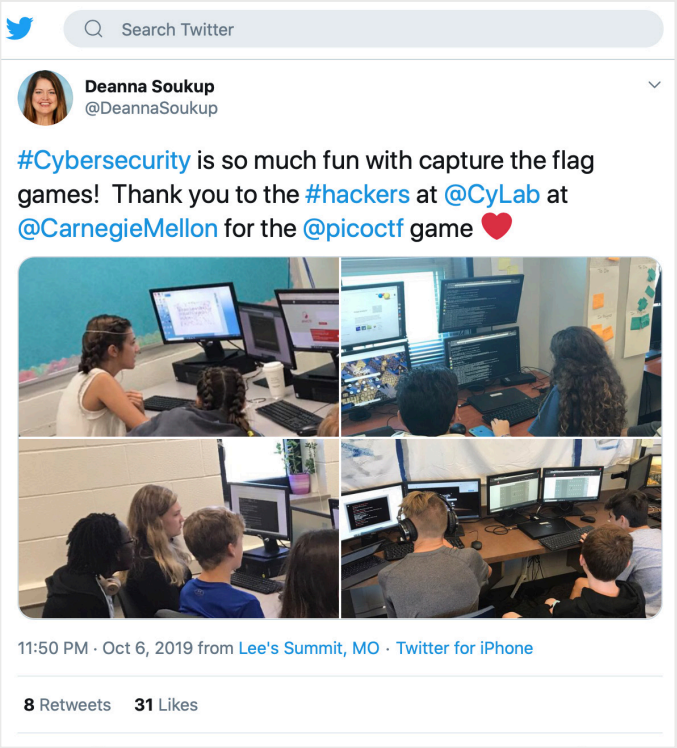
- Newark Academy, Livingston, NJ (2 members)
- Bridgewater-Raritan High School, Bridgewater Township, NJ
- Robinson High School, Tampa, FL
- Delaware Area Career Center, Delaware, OH

**4th place: hwcybsec - 34,201 points**

- Harvard-Westlake School, Studio City, CA

**5th place: dry roasted peanuts - 34,201 points**

- Liberal Arts and Science Academy, Austin, TX




# Provably-secure code incorporated into Linux kernel

Earlier this year, code from the provably correct and secure "EverCrypt" cryptographic library, which CyLab's Bryan Parno and his team helped develop and release last year, was officially incorporated into the Linux kernel — the core of the Linux operating system.

Specifically, the code's main use within the kernel is as part of Linux's latest built-in Virtual Private Network (VPN). Anyone using Linux – for example, anyone using the Android operating system, which is built on a modified version of Linux – can benefit from increased confidence in the VPN service.

"We're hopeful that some of the other components within the kernel will start using our verified code as well," said Parno, an associate professor of Electrical and Computer Engineering and Computer Science.

EverCrypt was originally released last year by a team consisting of researchers from Microsoft Research, Inria, and CyLab (Parno and his Ph.D. student Aymeric Fromherz). The cryptographic library is available for download on Github.

"With EverCrypt, we can rule out entire classes of vulnerabilities," says Parno. "We rule out memory safety vulnerabilities, correctness flaws, and we prove the implementations are resistant to some of the most popular types of side channel attacks."

"Side channel" attacks occur when an adversary is able to infer the secret key – a string of numbers that unlocks or decrypts encrypted data – simply by observing how an encrypted server responds to queries. For example, if the key is even, the server may respond faster than if the key is odd.

The encryption process takes time, of course, but Parno assures us that EverCrypt respects that.

"We've worked really hard on making sure EverCrypt's performance is at least as good as modern unverified cryptographic libraries," Parno says. "If your crypto is slow, anything you want to do securely will also be slow. EverCrypt isn't slow."

Pieces of the EverCrypt code set were already being used by Firefox, Microsoft, the Tezos blockchain, and the Linux Virtual Private Network, Wireguard. Parno and the rest of the EverCrypt team hope that other developers will continue to download their library and start test-driving it on their platforms.

EverCrypt is a part of Project Everest, a research initiative aimed at creating verifiably secure implementations of the HTTPS ecosystem, the foundation of secure Internet communications.

# Elaine Shi receives inaugural CyLab Distinguished Alumni Award

Elaine Shi, a CyLab alum and professor at Cornell University who will join the faculty at CMU this Fall, has been selected to receive the inaugural CyLab Distinguished Alumni Award for her "revolutionary" contributions to the field of cryptography and "pioneering" research in cryptocurrencies, according to her nomination. 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 grateful towards CMU and CyLab for having been selected to receive this great honor," says Shi.

The award will be presented to Shi at the 2020 CyLab Partners Conference in September.

"I am proud of the achievements of so many of our CyLab alumni and it is always fantastic to read about our alumni in the news or watch them – or their students – present at conferences," says CyLab director Lorrie Cranor. "CyLab created this annual award to publicly recognize some of our alumni who have had exceptional impact on the security and privacy field. I am thrilled to be presenting our first award to Elaine."

Shi was a computer science Ph.D. student in CyLab from 2003 to 2008. She was advised by CyLab's Adrian Perrig, and her thesis, "Evaluating Predicates over Encrypted Data," helped advance what's known as predicate encryption, which allows one to perform computations on encrypted data. This work led Shi towards improving what's known as Oblivious RAM, or ORAM.

ORAM helps protect encrypted data from a particular threat: adversaries may gain secrets from encrypted data by observing the patterns in which memory (RAM) is accessed when a program is executed on the data.

"Oblivious RAM is kind of like magic: it can encrypt the access patterns and the security is as strong as the encryption," Shi says. "Nothing is leaked."

The concept of ORAM was originally formulated in the 1980s, but suffered from its complexity, preventing it from being widely adopted in practice. Shi and her collaborators developed a novel paradigm for constructing ORAM which made it extremely simple, practical, and efficient.

"Previously, it was unthought of that something so simple could be done," says Shi. "Because of our work, it was possible to actually implement ORAM inside a secure processor."

Her work on ORAM attracted attention from various communities, with researchers implementing their algorithms in various applications. Notably, her paper, "Memory Trace Oblivious Program Execution," won the NSA Best Scientific Paper award for "building a bridge between cryptographic research and information flow research and showing how the latter can help us apply cryptographic advances in a principled and secure manner," and for "establishing a scientific foundation for the use of ORAM in programs."

Since 2011, Shi has been researching cryptocurrencies and blockchains. She co-authored the first peer-reviewed paper on Bitcoin, and the first peer-reviewed paper on decentralized smart contracts.

"Several of her pioneering papers, including the 'Bitter-to-Better' paper and her 'Hawk' privacy-preserving smart contract paper helped to shape the scientific foundations of this area," says Jun Zhao, a CyLab alumnus and an assistant professor of computer science and engineering at Nanyang Technological University. Zhao was one of Shi's two nominators, along with Shi's former Ph.D. advisor Adrian Perrig.

A recent line of her work has helped establish a new mathematical foundation of distributed consensus on a large scale.

"As a graduate student at CMU and in CyLab, it was the perfect environment. I was able to have a lot of intellectual freedom and pursue research that was cross-disciplinary combining theory and systems," Shi says. "I felt like I had the privilege to have the environment that CMU and CyLab were able to provide — it made all the difference. It's the best place to pursue a Ph.D. in security and cryptography."

This Fall semester, Shi will join the faculty at CMU with a joint appointment in Computer Science and Electrical and Computer Engineering.

# CyLab seminar series

Each year, CyLab holds a seminar series in the Fall and Spring semesters to give a platform for security and privacy experts to share their research with the CyLab community.

*Leemon Baird (left) and Hester Peirce (right) present at the CyLab seminar series.*

**SEPTEMBER 9, 2019**
**Peter Altabef**
*CEO, Unisys*
Title: NSTAC Cyber Moonshot

**SEPTEMBER 16, 2019**
**David Schwartz**
*CTO, Ripple*
Title: Under the Hood: XRP Ledger

**SEPTEMBER 30, 2019**
**Vibhaalakshmi (Vibhaa) Sivaraman**
*PhD Student, MIT*
Title: High-Efficiency Cryptocurrency Routing in Payment Channel Networks

**OCTOBER 14, 2019**
**Hester Pierce**
*Commissioner, SEC*
Title: Crypto Assets, Innovation and the Future of Financial Markets: A Fire-side Chat

**OCTOBER 28, 2019**
**Bo Li**
*Professor, University of Illinois*
Title: Secure Learning in Adversarial Environments

**NOVEMBER 4, 2019**
**Elaine Shi**
*Associate Professor, Cornell*
Title: Rethinking Large-Scale Consensus

**NOVEMBER 11, 2019**
**Kathleen Carley**
*Professor, CMU*
Title: BEND maneuvers using Bots and Memes for Social Cybersecurity

**NOVEMBER 18, 2019**
**Adam Aviv**
*Associate Professor, George Washington University*
Title: Human Factors in Mobile Authentication

**NOVEMBER 25, 2019**
**Leemon Baird**
*Founder and CTO Hashgraph*
Title: Scaling up DLTs

**DECEMBER 2, 2019**
**Patrick McDaniel**
*Professor, PSU*
Title: The Challenges of Machine Learning in Adversarial Settings

**JANUARY 27, 2020**
**Angela Walch**
*Professor, St. Mary's*
Title: Intermediaries Who Must Not Be Named? A Legal & Policy Research Agenda for Crypto Miners

**FEBRUARY 3, 2020**
**Steve Lipner**
*Executive Director, Safecode.org*
Title: Lessons Learned – Fifty Years of Mistakes in Cybersecurity

**FEBRUARY 24, 2020**
**Conrad Tucker**
*Professor, CMU*
Title: From Generative Neural Networks to Social Media Networks: Ascertaining the Veracity and Security of Data in the Information Age

**JUNE 19, 2020**
**Raluca A. Popa**
*Assistant Professor, UC-Berkeley*
Title: Towards a secure collaborative learning platform

# 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.

### Undergraduate Minor in Information Security, Privacy, and Policy

The Undergraduate Minor in Information Security, Privacy, and Policy is launching in Fall 2020 and will offer 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.

**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.
- 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.*

- PhD 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.


*Right: Shikun "Aerin" Zhang, a Ph.D. student in the School of Computer Science's Language Technologies Institute, presents her research at the annual "Data Privacy Day" celebration, which is hosted by MSIT-PE graduate students.*

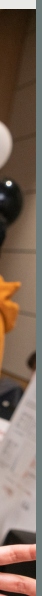
# CyLab executive education offerings

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.



# 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)

**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**
*Research and teaching scientist*, INI

**Jason Hong**
*Professor*, Human-Computer Interaction Institute

**Limin Jia**
*Associate research professor*, ECE, INI

**Timothy Libert**
*Special faculty instructor*, ISR

**Piotr Mardziel**
*Systems scientist*, ECE

**Aleecia McDonald**
*Assistant professor of the practice*, INI

**Javad Mohammadi**
*Special faculty, ECE*

**Bryan Parno**
*Associate professor*, CSD, ECE

**Corina Pasareanu**
*Senior 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

**Maverick Woo**
*Systems scientist*, CyLab

**Osman Yagan**
*Associate research professor*, ECE

**Ding Zhao**
*Assistant professor*, Mechanical Engineering, Robotics Institute

# Featured speaking engagements by faculty


*CyLab's Lorrie Cranor gave a keynote talk about password security at RSA 2020. The talk served as a warm-up act for magician duo Penn & Teller who performed an elaborate magic trick involving passwords.*

**Alessandro Acquisti:**

- Keynote at the IAPP Europe Data Protection Congress. November 2019.
- Keynote at Purdue 2050: Conference of the Future, Purdue University. November 2019.

**Jonathan Aldrich:**

- "Usability Evaluation of the Obsidian Smart Contract Language." Science of Security Lablet PI meeting. January 2020.

**Lujo Bauer:**

- "AI in cybersecurity: New defenses and new dangers." CMU-Africa seminar. October 2019.
- Keynote: "The promise and threat of AI for cybersecurity." German American Chambers of Commerce East Coast Industry Forum. October 2019.
- "AI in computer security: New defenses and new dangers." ETH Zurich. November 2019.
- "On the susceptibility to adversarial examples under real-world constraints," invited talk, ICLR 2020 Workshop: "Towards Trustworthy ML: Rethinking Security and Privacy for ML." April 2020.

**Shawn Blanton:**

- Three talks on "Designing Secure Hardware Systems":
  - 2019 Workshop on Future Computing. December 2019.
  - Lockheed Martin Distinguished Seminar. February 2020.
  - NYU ECE Seminar Series. March 2020

**Yang Cai:**

- Four talks at the lecture series of "Engineers Respond to COVID-19" hosted by IEEE Pittsburgh, April-May 2020:
  - "Remote Fever Screening"
  - "Haptic Interfaces"
  - "Local COVID-19 Data Collection and Modeling"
  - "Reopen and Renaissance"

**Kathleen Carley:**

- Keynote: "Social Cybersecurity and the Pandemic." ICWSM. June 2020.
- Keynote: "CUES - Understanding information maneuvers in social media using implicit information." TextXD: Text Analysis across Domains. December 2020.
- Keynote: "Artificial Intelligence and Social Cybersecurity." AAAI Symposium on AI in Government and Public Sector. November 2019.
- "Influence Campaigns in Social Media," Plenary speaker. Hacking Democracy: Influence operations in the Digital Age. February 2020.
- "Influence Operations: BEND maneuvers using bots and memes for social cybersecurity." Plenary speaker. The NATO Science for Peace and Security Programme: Senior Leadership Roundtable on Information-Related Hybrid Threats in South East Europe. October 2019.

**Nicolas Christin:**

- "The dark web isn't that dark." TTI/ Vanguard Ubiquitous AI. June 2020.
- "A deep dive in the deep web: Insights from eight years of online anonymous marketplaces measurements." Invited talk. American Association of University Women (AAUW). October 2019.
- "A deep dive in the deep web: Insights from eight years of online anonymous marketplaces measurements." Invited colloquium. University of Wisconsin-Madison, Computer Science Department. September 2019.
- "A deep dive in the deep web: Insights from eight years of online anonymous marketplaces measurements." Invited talk. Virtual Currency Symposium. September 2019.

**Lorrie Cranor:**

- Keynote: The Hugh Thompson Show, featuring Penn & Teller and Dr. Lorrie Cranor. RSA Conference. February 2020.
- Keynote: "Security and Privacy for Humans." CyberCorps Scholarship for Service (SFS) 2020 Annual Job Fair and Symposium. January 2020.
- "Privacy notice and consent for a GDPR/CCPA/IoT world." Harvard

Business School Digital Seminar Series. February 2020.

- "Security and Privacy for Humans." University of Minnesota Cray Distinguished Speaker Series. November 2019.
- Cofounded with alumnus Lea Kissner (and serving as program co-chair) USENIX Conference on Privacy Engineering Practice and Respect, which took place in August 2019.

**Virgil Gligor:**

- Keynote: "Winning Against any Adversary on Commodity Computer Systems." ACM, International Workshop on the Cyber Arms Race. November 2019.
- Keynote: "Establishing and Maintaining Root of Trust on Commodity Computer Systems." ACM ASIACCS. July 2019.

**Dena Haritos Tsamitis:**

- "Snap Out of It: Overcoming the Imposter Syndrome." ACM Richard Tapia Celebration of Diversity in Computing. September 2019.
- "Breaking Down Professional Boundaries: Group Mentoring." Strong Women Strong Girls (SWSG). November 2019.

**Hanan Hibshi:**

- "Decision Support for Cybersecurity Risk Assessment." Invited Speaker. TaCS_CRISMA (Clinical Science Program, The CRISMA Center) Research Group at University of Pittsburgh, Department of Critical Care Medicine. February 2020.
- "Addressing the Shortage in Cyber Security Talent." Invited Speaker. Deloitte Services LP. July 2019.
- "Uber Day of Security INI Capture-the-Flag Workshop." Facilitator. Uber Advanced Technologies Group (ATG). October 2019.

**Swarun Kumar:**

- "The future of wireless is connecting everyday objects." TEDxPittsburgh. July 2019.

**Tim Libert:**

- "Can the Platforms Save Us? The Strengths and Limits of the Private Sector." Invited panelist. Conference on New Media and Democracy. November 2019.

**Aleecia McDonald:**

- "Elections, Privacy, & The Public Trust." Moderator. SCC Data Privacy Day. January 2020.
- With Patrick Tague: "Practicum: Bridging the Gap Between Theory and Practice in Cybersecurity." National Initiative for Cybersecurity Education (NICE) Conference. November 2019.
- "Protecting Your Privacy: The California Consumer Privacy Act." Saratoga Library. July 2019.

**Bryan Parno:**

- Keynote: "Developing High-Performance Mechanically-Verified Cryptographic Code. Workshop on Foundations of Computer Security. June 2020.
- "Developing High-Performance Mechanically-Verified Cryptographic Code." Invited Talk. IACR Conference on Cryptographic Hardware and Embedded Systems. August 2019.

*CyLab's Tim Libert speaking at Tufts University for the Conference on New Media and Democracy.*

**Jon Peha:**

- Keynote: "Spectrum Policy for Intelligent Transportation Systems." 19th IEEE Wireless Telecommunications Symposium. April 2020.
- "What 5G Cannot Solve and the Need for 6G." IEEE DySPAN. November 2019

**Norman Sadeh:**

- Served on the "Online Privacy + Security Forum" panel on IoT Privacy in the Age of CCPA and GDPR with Achim Klabunde (Advisor to the European Data Protection Supervisor) and Gabriela Zanfir-Fortuna (Senior Policy Counsel, Future of Privacy Forum). May 2020.
- Tutorial: "Contextual Integrity: From Theory to Practice." SOUPS 2019. August 2019.

**Robert Schiela:**

- "Quality Assurance and Coding Standards for Parallel Software." SC19 International Conference for High Performance Computing, Networking, Storage, and Analysis. November 2019.

**Mark Sherman:**

- "Using AI to Build More Secure Software." Abstractions Conference. August 2019.
- "Growing Risks in the Software Supply Chain." 2019 Platform Security Summit. October 2019.
- "Using AI to Build More Secure Software." Global Data Conference. January 2020.

**Carol Smith:**

- "Designing Trustworthy AI: A User Experience (UX) Framework." RSA Conference 2020. February 2020.

**Carol Woody:**

- "Think like a hacker: a look at the state of cybersecurity." Tech Day at William and Mary. November 2019.

# Featured grants

**Alessandro Acquisti and Lorrie Cranor**

- "Public Privacy Protective Behaviors." Funder: NortonLifeLock

**Lujo Bauer, Zico Kolter, Matthew Fredrikson, Corina Pasareanu, and Pradeep Ravikumar**

- "Provably Robust Deep Learning." Funder: DARPA

**Shawn Blanton, Ken Mai and Larry Pileggi**

- "Split Chip Desgn for Obfuscation and IC Trust." Funder: DARPA

**Shawn Blanton and Larry Pileggi**

- "Developing and characterizing the Latch-based Logic Locking design methodology." Funder: Kansas City Nuclear Security Campus

**Yang Cai:**

- "Learn-On-The-Fly for Small UAVs." Funder: Northrop Grumman Corporation
- "Cyber Attribution with Dynamic Graphs." Funder: Northrop Grumman Corporation
- "Smart Glasses for Improving Mobility of Low Vision People." Funder: Mobility21 National USDOT UTC for Mobility of Goods and People
- "AI for Vulnerability Screening." Funder: Siemens
- Lee Trawick, Cai's Ph.D. student, received a Siemens FutureMaker Fellowship, 2019-2020

**Lorrie Cranor:**

- "Identifying User Needs for Advertising Controls." Funder: Facebook
- "Usable Consent and Authorizations for Digital Healthcare Channels." Funder: Highmark Health

**David Garlan:**

- "Autonomy for Robotics Platforms." Funder: Software Engineering Institute

**Dena Haritos Tsamitis:**

- "Department of Defense Cyber Scholarship Program." Funder: Department of Defense

**Dena Haritos Tsamitis (PI) and Hanan Hibshi (Co-PI):**

- "Improving Security of Open Source Digital Identity Software." Funder: Bill & Melinda Gates Foundation

**Hanan Hibshi and Patrick Tague:**

- "NIAP Reference Mobile Apps & Developer Training." Funders: NOWSECURE, INC. (VIAFORENSICS)

**Jason Hong:**

- "Social interactions, social connectedness, and health outcomes during the COVID-19 pandemic." Funder: NSF
- "Designing Alternative Representations of Confusion Matrices to Evaluate Public Perceptions of Fairness in Machine Learning." Funder: Amazon
- "Evaluating People's Perceptions of Fairness in Machine Learning." Funder: Block Center for Technology and Society

**Javad Mahammadi:**

- "Investigating and mitigating the impact of communication disruption on the coordination and operation of Internet of Things (IoT) connected Distributed Energy Resource (DER)s and power systems operation." Funder: State of PA via Engineering Research Accelerator. Co-PI: Osman Yagan

**Bryan Parno:**

- "Verified Transformations for Automated Hardware-Specific Optimization." Funder: Intel

**Norman Sadeh:**

- "Work on personalized privacy assistants." Funder: Mozilla
- "Digital Assistants to automatically answer people's privacy questions." Funder: NSF

**Justine Sherry, Rashmi Vinayak, Christos Faloutsos, and David Garlan:**

- "Adaptive, Intelligent, and Distributed Assurance Platform." Funder: CMU Portugal

# Featured recognitions

Five CMU security and privacy papers were awarded IEEE's Test of Time award. The CMU authors included Haowen Chan, Virgil Gligor, Thomas Longstaff, Bryan Parno, Adrian Perrig, and Dawn Song. To learn more, read story on page 7.

Three women in CyLab — Grace Liu, Soo-Jin Moon, and Elahe Soltanaghaei — were invited to an exclusive visit to Facebook's data center to discuss network research.

**Javad Mohammadi and Soummya Kar:**

- A team they were part of placed in the top 10 in all divisions of the Advanced Research Projects Agency-Energy (ARPA-E) Grid Optimization (GO) Competition. The competition results were announced recently by the U.S. Department of Energy Secretary

**CyLab Passwords group:**

- A team of CyLab faculty and graduate students received the Allen Newell Award for Research Excellence for their pioneering contribution to the science of evaluating password strength and creating state-of-the-art tools that enable individuals and groups to more easily secure their systems. Team members included CyLab's Lujo Bauer, Nicolas Christin, and Lorrie Cranor; and CMU alumni Saranga Komanduri, Michelle Mazurek, William Melicher, Sean Segreti, Rich Shay, and Blase Ur

**Alessandro Acquisti:**

- Named Endowed chair: Trustees Professor of Information Technology and Public Policy, 2020
- Received the 2019 AIS College of Senior Scholars Award for the paper, "Beyond the privacy paradox: Objective versus relative risk in privacy decision making." ICIS, 2019
- Received the 2019 MISQ Best paper Award for the paper, "Beyond the privacy paradox: Objective versus relative risk in privacy decision making." ICIS, 2019

**Mary Ann Blair:**

- Won the CISO of the Year Award for the education/nonprofit category during the Pittsburgh Tech Council's annual CIO of the Year Awards

**Yang Cai:**

- Received a First Place Award at the NIST Haptic Interfaces for Public Safety Challenge. November 2019
- Received a Best Paper Award for a paper titled, "Activity Recognition from Sensor Fusion from Helmet." CSIP-BMEI, 2019

**Kathleen Carley:**

- Received a Best Late Breaking Paper award at SBP-BRiMS 2019 for the paper, "Detecting malware communities using socio-cultural cognitive mapping"

**Lorrie Cranor:**

- Elected to Computing Research Association Board of Directors, 2019-2022
- Appointed to Consumer Reports Digital Lab Advisory Council

**Giulia Fanti:**

- Received a JP Morgan Chase Faculty Research Award (with Vyas Sekar) on "Privacy-Preserving Generation of Synthetic Time Series Data"
- Received a Google Faculty Research Award (with Sewoong Oh @ University of Washington) on "Disentangling Generative Models for Federated, Identity-Sensitive Representation Learning"

**David Garlan:**

- Received the Most Influential Paper award at SEAMS 2020 for Impact and Professional Merit for the paper, "Architecture-based Self-adaptation in the Presence of Multiple Objectives

**Coty Gonzalez:**

- Received a Best Paper Award for a paper about cyber deception at the HICSS conference. January 2020

*Gonzalez's co-authors (L-R), Palvi Aggarwal and Edward Cranford, show off their Best Paper Award at HICSS.*

**Jason Hong:**

- Elected to the CHI Academy, an honorary group of individuals who have made substantial contributions to the field of human-computer interaction
- Received a 2019 Amazon Research award for his research titled "Designing Alternative Representations of Confusion Matrices to Evaluate Public Perceptions of Fairness in Machine Learning"

**Swarun Kumar:**

- Received NSF CAREER award. January 2020
- Received a Best Paper Honorable Mention and Best Demo for a collaboration with Anthony Rowe at ACM MobiSys 2020. June 2020
- Received a Best Paper Award for a collaboration with Anthony Rowe and Bob Iannucci. April 2020

**Claire Le Goues:**

- Received an ACM SIGSOFT Early Career Researcher Award for groundbreaking work on automated program repair, impact on industrial practice, and service to the software engineering research community

**Bryan Parno:**

- Received a Distinguished Paper Award, ACM PLDI Conference, 2020
- Received the Joel and Ruth Spira Excellence in Teaching Award for 2019-2020

**Marios Savvides:**

- Received the 2020 AI Excellence Award for his role as Chief AI Scientist at Bossa Nova Robotics
- The Army Research Lab identified Savvides as an "Outstanding AI Contributor" that has advanced the impact of AI for the US Army

**Justine Sherry:**

- Named to the Information Science and Technology (ISAT) Study group
- Sherry's Ph.D. student Ranysha Ware received a 2020 Applied Networking Research Prize (ANRP) from the Internet Engineering Task Force

**Virginia Smith:**

- Received a Facebook Faculty Award for work titled, "*Private Federated Learning: Differential Privacy in Heterogeneous Networks*" in May 2020, along with CMU faculty member Ameet Talwalkar

**Carol Woody:**

- Received the 2019 Information Security Leadership Award (ISLA) from $(ISC)^2$ – the world's largest nonprofit association of certified cybersecurity professionals

# 2020 CyLab Presidential Fellows

### Akshay Gadre

**(ECE, advisor: Swarun Kumar)**

Gadre's research focuses on providing security benefits to clients of low-power wide-area networks (LP-WAN), who are incapable of achieving security and privacy in their communications because adversaries are orders of magnitude more powerful than low-power clients.

### Danielle Duvalsaint

**(ECE, advisor: Shawn Blanton)**

Duvalsaint's research focuses on the threats in hardware that can result from outsourcing portions of the integrated circuit design. Her work aims to mitigate these threats by creating security metrics which assess the effectiveness of hardware security design methodologies.

### Mansi Sood

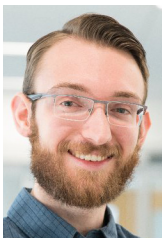
**(ECE, advisor: Osman Yagan)**

Sood's research focuses on demystifying the role of structural properties of a network on the achievable performance in security-critical networked applications such as wireless sensor networks, cryptocurrency networks and multi-party computations.

### McKenna McCall

**(ECE, advisor: Limin Jia)**

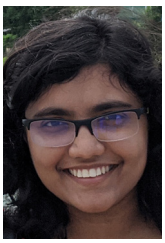
McCall's research involves information flow security, which ensures that secret information is not unintentionally leaked to malicious parties, and also prevents these parties from manipulating trusted components of a system.



### Peter Story

**(ISR, advisor: Norman Sadeh)**

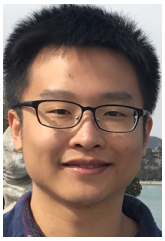
Story's research focuses on helping people translate their intention to protect their security and privacy into action. In particular, he studies the effects of educational interventions based on protection motivation theory and implementation intentions.



### Sanghamitra Dutta

**(ECE, advisor: Pulkit Grover)**

Dutta's research focuses on a rigorous quantification of bias in machine learning with respect to gender, race, etc., that enables one to check if the bias arose purely due to business necessities, drawing inspiration from the business necessity defense in the disparate impact law.



### Zinan Lin

**(ECE, advisors: Giulia Fanti and Vyas Sekar)**

Lin proposes to develop high-fidelity and privacy-preserving data sharing systems with generative adversarial networks (GANs), so as to lower the barrier of data sharing and unleash the potential of data-driven research.

# Graduated Ph.D. students

**Michael J. Coblenz, Ph.D. in Computer Science**
Advisors: Jonathan Aldrich and Brad Myers
Thesis title: User-Centered Design of Principled Programming Languages
Defense: May 2020

**Pardis Emami-Naeini, Ph.D. in Societal Computing**
Advisors: Lorrie Cranor and Yuvraj Agarwal
Thesis title: Informing Privacy and Security Decision Making in an IoT World
Defense: May 2020
Current position: Postdoc at University of Washington

**Bin Liu, Ph.D. in Computer Science**
Advisor: Norman Sadeh
Thesis title: "Can Machine Learning Help People Configure their Mobile App Privacy Settings?"
Defense: December 2019
Current position: Google

**Ashutosh Pandey, Ph.D. in Software Engineering**
Advisor: David Garlan
Thesis title: Hybrid Planning in Self-adaptive Systems
Defense: December 2019
Current position: Facebook

**Mahmood Sharif, Ph.D. in ECE**
Advisors: Nicolas Christin, Lujo Bauer
Thesis title: Practical Inference-Time Attacks Against Machine-Learning Systems and a Defense Against Them
Defense: November 2019
Current Position: VMWare Research Group postdoc, joining Tel Aviv University as senior lecturer in 2021

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

**Zeye Liu**
**Advisor: Shawn Blanton**
Thesis title: A Test Chip Design for Automatic Insertion of Logic Circuit Demographics
Defense: March 2020
Current position: Intel Engineer

# Featured CyLab media mentions

The Telegraph

OCT 27, 2019

## CyLab's Sherry comments on Internet fairness findings

New research out of Carnegie Mellon shows that Google's new congestion control algorithm, named BBR, hogs Internet traffic, even when other services are vying for connections. "By any traditional version of [network] fairness, BBR is not fair," **Justine Sherry** said. The researchers believe that the algorithm will likely change as a result of their findings.

The New York Times

NOV 18, 2019

## CyLab's Sekar warns about "juice jacking"

As a busy holiday travel season approaches, law enforcement agencies are warning about "juice jacking," the latest way criminals can hack your accounts. Juice jacking occurs when unsuspecting users plug their devices into USB ports or use USB cables that contain malware. **Vyas Sekar** told the The *New York Times* that "there is a risk" in charging your devices at public charging stations.

WIRED

NOV 25, 2019

## Fanti comments on making cryptocurrencies private

So-called "privacy coins" are gaining popularity right now, as Bitcoin has been shown to not be as clandestine as once thought. But even these privacy coins have their own flaws, points out **Giulia Fanti**. She says that Mimblewimble, a technology designed for cryptocurrencies to increase privacy, has its own vulnerabilities.

abc NEWS

DEC 4, 2019

## Telang warns about email phishing over the holidays

While cybercriminals are a threat year-round, they're particularly active around the holidays. Phishing attacks are particularly prevalent during the holiday season, and **Rahul Telang** explained to ABC News that employees often feel a responsibility to read an email that is realistic enough, but this can lead to trouble. "It might not sound very personal, but you have an idea that you should go ahead—you feel like the email is coming from the boss," he says.

BBC

FEB 5, 2020

## Libert quoted on privacy

**Timothy Libert** was quoted by the BBC about privacy issues in the UK. "I've been a web developer since the late 1990s and a privacy researcher for the past seven years and this may be the most unexpected place I've seen an ad online," said Libert.

c|net

FEB 19, 2020

## Sadeh launches new privacy app and infrastructure

**Norman Sadeh** was featured in a number of outlets -- CNET, Engadget, VICE, Gizmodo, and Mashable, to name a few -- after the launch of the IoT Assistant app and infrastructure that he and his team developed. According to Sadeh, "... research has shown that most people have little awareness about the amount of data collected today by IoT technologies."

USA TODAY

MAR 19, 2020

## Carley identifies three types of misinformation during COVID-19 outbreak

As the COVID-19 pandemic works its way around the world, mis- and dis-information about the disease has been deployed "to incite panic and sow confusion," **Kathleen Carley** told USA Today.

IEEE SPECTRUM

APR 9, 2020

## Peha comments on routing practices

A battle over call routing practices heats up as demand for conferencing services stress telephone networks: "I think the FCC may need to reconsider (closing certain loopholes) in the middle of a pandemic that's forcing people to work from home," says **Jon Peha** to *IEEE Spectrum*.

THE WALL STREET JOURNAL.

JUN 14, 2020

## Bauer quoted on data privacy

**Lujo Bauer** was quoted in *The Wall Street Journal* on a new messaging app called Signal. The app doesn't log much information (metadata) about the nature of the messages themselves. "Signal makes it a point to keep as little data as possible while still being able to provide service," said Bauer.

CR Consumer Reports

JUN 24, 2020

## Cranor quoted on iPhone privacy

**Lorrie Cranor** was quoted in *Consumer Reports* on Apple's new privacy features. "Our research has found that app developers tend not to know much about privacy, and many of them don't work for big companies where there are lawyers or privacy engineers to help them," Cranor says.

# 2019 CyLab Partners Conference and 15-year anniversary

At last year's CyLab Partners Conference, dozens of CyLab researchers presented their latest research findings to representatives from the CyLab Partners Program. At the conclusion of the conference, attendees celebrated 15 years since the original creation and launch of CyLab at Carnegie Mellon University.


1

2


3

4

5


6

7

8

9

10

1. *Yuvraj Agarwal presents his research at the CyLab Partners Conference.*
2. *Miao Yu, a postdoctoral researcher in CyLab, attends the CyLab Partners Conference poster session.*
3. *Conference attendees enjoyed CyLab cookies in celebration of CyLab's 15-year anniversary.*
4. *Aymeric Fromherz presents his research at the CyLab Partners Conference poster session.*
5. *Patrick Tague chats with attendees at CyLab's 15-year anniversary celebration.*
6. *Lujo Bauer (left) presents his research on fooling AI systems at the CyLab Partners Conference. Bauer's former Ph.D. student, Mahmood Sharif (right), is shown on the slide displaying his facial recognition thwarting eyeglass frames.*
7. *Ritwik Gupta presents his research at the CyLab Partners Conference.*
8. *Michael Lisanti (right), director of Partnerships for CyLab, raises his glass during a toast at CyLab's 15-year anniversary celebration.*
9. *Grace Liu, a postdoctoral researcher in CyLab, presents her research at the CyLab Partners Conference poster session.*
10. *(L-R) Lorrie Cranor, Hanan Hibshi, and Dena Haritos Tsamitis pose for a group photo at the CyLab 15-year anniversary celebration.*

# Partners shaping a safer future

Carnegie Mellon CyLab is a world leader in innovative thinking and game-changing collaborations that make life more 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 defense agencies in the USA and international partner countries. Every partnership is united by a passion to create a world in which technology can be trusted.

To work together to come up with a collaboration plan that benefits your team and CyLab, contact Michael Lisanti, Director of Partnerships, mlisanti@cmu.edu or +1 412 268 1870

Acronis
aetna
AT&T
aws
BOEING
DSO NATIONAL LABORATORIES
DSTA Defence Science & Technology Agency
EATON Powering Business Worldwide
facebook
IBM
infineon
leidos
LG Electronics
LOCKHEED MARTIN
Microsoft
MITSUBISHI HEAVY INDUSTRIES
National Police Agency JAPAN
NATO HQ C3 Staff
NOKIA Bell Labs
NORTHROP GRUMMAN
RESILIENCE JAPAN
SailPoint
Sandia National Laboratories
SIEMENS Ingenuity for life
T-Mobile
TRANE TECHNOLOGIES
UPMC LIFE CHANGING MEDICINE

# CyLab news briefs over the past year

**SEP10**

**CyLab's Corina Pasareanu and colleagues receive $1.2 million grant to develop automated bug-finding techniques**

The National Science Foundation has awarded a $1.2 million grant to researchers at Carnegie Mellon University, UC-Berkeley, and UC-Santa Barbara to develop automated bug-detection and repair techniques that work at large scales.

**SEP25**

**Protecting 3D printers from attackers**

CyLab's researchers developed a tool to identify security risks of networked 3D printers.

**SEP26**

**CyLab launched the largest hacking competition in history**

CyLab launched the sixth iteration of picoCTF, a free, online cybersecurity competition aimed at middle and high school students.

**OCT04**

**This new tool for developers can help preserve app users' privacy**

A team of CyLab researchers created a tool that nudges developers to think a bit harder about user privacy when coding data requests.

**OCT18**

**New tool gives researchers a better look at online anonymous marketplaces**

In a study presented at the Knowledge Discovery and Data (KDD) Mining Conference, former CyLab Ph.D. student Xiao Hui Tai teamed up with two other researchers to develop an algorithm that will help law enforcement agencies crack down on illicit products being sold on online anonymous marketplaces.

**NOV11**

**CMU women prominent among Rising Stars 2019**

Women from Carnegie Mellon University outnumbered those from every other institution at Rising Stars 2019, an annual workshop for early-career women in computer science and electrical and computer engineering. Two women from CyLab also won two of the four prizes in the workshop's Research Pitch Competition.

**NOV15**

**CyLab researchers propose new rules for Internet fairness**

Just weeks after a team of Carnegie Mellon researchers showed that Google's new congestion control algorithm (CCA) was giving an unfair advantage to its own traffic over services using legacy algorithms, the same team proposed new guidelines on how future algorithms should be developed.

**NOV22**

**Sharing accounts in the workplace is a mess**

In a new study, CyLab researchers found that people in the workplace are sharing accounts like Facebook, Google, and company email accounts for a variety of reasons. The way they share these accounts could lead to mishaps.

**JAN02**

**Using AI to recycle bottles**

A collaborative project in partnership with CMKL University aims to develop an artificial intelligence (AI) system to accurately screen bottles for reuse and recycling.

**JAN08**

**Cybercriminals: Things are about to get a lot more confusing for you**

Two papers on cyber deception authored by CyLab's Cleotilde Gonzalez and colleagues are being presented at this week's Hawaii International Conference on System Sciences (HICSS).

**JAN23**

**"Hacked! An Escape Room Experience" puts you in cybercriminals' shoes**

"Hacked! An Escape Room Experience" gave participants an "Escape Room"-like experience in which they took on the role of cybercriminal to solve a series of challenges.

**JAN30**

**Safety helmet for fire fighters**

Communication technologies built into a firefighter's helmet can send directional information in realtime to firefighters working in dangerous environments.

**FEB11**

**The curious case of OpenBazaar**

CyLab's Nicolas Christin and graduate student James Arps presented the first in-depth look at the decentralized online anonymous market known as OpenBazaar.

**FEB19**

**New infrastructure will enhance privacy in today's Internet of Things**

A team of Carnegie Mellon researchers launched the IoT Assistant, an app that informs users about what IoT technologies are around them and what data they are collecting. An accompanying cloud-based portal allows IoT owners to register their devices to the infrastructure.

**FEB21**

**Elite high school hackers convene at CMU to claim their well-earned picoCTF prizes**

Last week, the top three winning teams from picoCTF 2019 visited Carnegie Mellon to receive their prizes.

**MAR02**

**To predict an epidemic, evolution can't be ignored**

In a new study, a team of Carnegie Mellon University researchers show for the first time how important evolutionary adaptations are in predicting epidemics.

**MAR06**

**CMU's big showing at RSA 2020**

The Human Element" was the theme of this year's RSA Conference in San Francisco, which featured CyLab Director Lorrie Cranor talking about usable security research as a warm-up act for magician duo Penn & Teller.

**MAR16**

**Why people delay software updates, despite the risks**

In a study published in the latest issue of the Journal of Cybersecurity, a team of CyLab researchers found that the time-cost of updates and individuals' risk preferences have a significant impact on whether or not a user applies a software update, and how long it takes them to do so.

**MAR26**

**Q&A with Kathleen Carley**

Amid the coronavirus pandemic, disinformation about the virus is spreading at lightning speeds. CyLab's Kathleen Carley has been monitoring the situation.

**APR14**

**Managing necessary bias in AI**

Some biases in AI might be necessary to satisfy critical business requirements, but how do we know if an AI recommendation is biased strictly for business necessities and not other reasons?

**APR29**

**Provably-secure code incorporated into Linux kernel**

This month, code from the provably correct and secure "EverCrypt" cryptographic library, which CyLab's Bryan Parno and his team helped develop and release last year, was officially incorporated into the Linux kernel — the core of the Linux operating system.

**APR30**

**Yağan receives emergency NSF grant to help fight COVID-19**

ECE's Osman Yağan seeks to understand the spread of coronavirus and how public health measures can reduce that spread.

**APR30**

**Online status indicators during a pandemic: do they work?**

People working from home have been using online status indicators to check whether their co-workers are available, but recent CyLab research shows that these indicators lead to some strange behaviors.

**MAY18**

**Remote fever-scanning technologies**

Researchers are developing affordable fever-screening technologies for buildings and first responders to detect fevers, using an algorithm to detect faces and measure temperature on the forehead.

**MAY22**

**Passwords research group awarded the 2020 Allen Newell Award for Research Excellence**

A group of CyLab faculty and graduate students were just awarded the Allen Newell Award for Research Excellence for their contributions from a decade of passwords research.

**MAY26**

**After a breach, users rarely change their passwords, and when they do, they're often weaker**

A recent study authored by CyLab researchers shows that only a minority of people change their passwords after a security breach, and those that do often change them to weaker ones.

**JUN03**

**Justine Sherry named to ISAT Study Group**

The Defense Advanced Research Projects Agency (DARPA) has named CyLab's Justine Sherry to the Information Science and Technology (ISAT) Study Group for a three-year term beginning this summer.

**JUN11**

**Finding privacy choices on websites is hard for average users. Don't blame them; experts also find it hard.**

In a study presented at this year's ACM CHI conference, CyLab researchers show precisely how difficult it is for average users to access privacy choices online.

**JUN18**

**How much control are people willing to grant a personal privacy assistant?**

In a new study presented at the CHI 2020 conference, CyLab researchers sought to find out how much autonomy people would feel comfortable giving to a personalized privacy assistant.

**JUN25**

**Shedding light (and sound) on hidden IoT devices in your next hotel room**

In a new study, a team of CyLab researchers explored different locator designs to make IoT devices seem a little less hidden.

**JUL24**

**Three CyLab papers presented at the FTC's PrivacyCon2020**

Three CyLab papers were presented at this year's PrivacyCon, focusing on privacy and security nutrition labels, making privacy choices easier, and perceptions of advanced video analytics.

**JUL29**

**New programming language and tool ensures code will compute as intended**

A team of researchers including CyLab's Bryan Parno published a study about a new tool that mathematically proves that concurrent programs will compute correctly.

**AUG10**

**Carnegie Mellon hacking team finishes 2nd at DefCon**

Carnegie Mellon University's competitive hacking team, the Plaid Parliament of Pwning (PPP), finished in 2nd place in the "Capture the Flag" competition—widely referred to as "The Olympics of Hacking"—at this year's DefCon security conference.

**AUG14**

**What if you could better control what mobile apps do with your data?**

Researchers in CyLab are working to create digital "privacy assistants" that can recommend phone app privacy settings to users based on their preferences.

**AUG18**

**Simple "nudges" can encourage people to use a safer payment method**

A team of CyLab researchers found two forms of "nudging" that can successfully convince people to start using mobile payment, which is more secure than paying with a credit card at a point-of-sale terminal.

**AUG21**

**Home automation rules are more risky and less risky than we thought**

A CyLab study found that previous risks in home automation rules aren't as dangerous in reality as once thought, but new threats were identified.


*In January we welcomed Bill Sanders (2nd row, wearing a tie) as the new dean of our College of Engineering as well as a CyLab faculty member. Bill's research interests include secure and dependable computing, with a focus on critical infrastructure. We took a group photo when Bill joined us for a town hall meeting with some of our CyLab students, faculty, and staff.*

CyLab Carnegie Mellon University
Security and Privacy Institute