CYLAB 2018-2019 YEAR IN REVIEW

CyLab Carnegie Mellon University
Security and Privacy Institute

Letter from the Director

DEAR FRIENDS

I would like to introduce myself and share with you CyLab's 2018-19 year in review, which includes a brief reflection on the first 15 years of CyLab. I joined the Carnegie Mellon faculty at the end of 2003, shortly after the launch of CyLab. Fifteen years later, I was appointed director of CyLab in January 2019. So both CyLab and I celebrated 15 years at CMU this year.

Over the past 15 years, CyLab has become the preeminent interdisciplinary academic security and privacy institute. CyLab currently includes about 30 core faculty and another 80 affiliated faculty, plus staff, postdocs, and students. We have faculty from across the university, including those with appointments in several departments in the School of Computer Science and the College of Engineering, Social and Decision Sciences, Philosophy, Heinz College, Tepper School of Business, the Information Networking Institute, and the Software Engineering Institute. While most of our faculty are in Pittsburgh, we also have faculty at our Silicon Valley, Qatar, and Africa campuses. In addition, CyLab partners with about two dozen external organizations, including companies and government agencies that have joined our growing partnership program.

One of CyLab's greatest strengths is our collaborative, interdisciplinary approach to security and privacy research and education. We are the epicenter of usable privacy and security research (which is my personal focus), with collaborations across the university. In addition, with CMU's strength in artificial intelligence, we have become a leader in research at the intersection of security and AI, including adversarial machine learning and cyber autonomy. These are just a couple of the many examples of collaborative research at CyLab. Going forward, we will continue to provide research support, seed funding, and a welcoming collaborative environment to encourage more innovative interdisciplinary research.

CyLab faculty have launched many innovative and unique educational programs in the security and privacy space. CMU offers masters programs in information security, security policy and management, and privacy engineering, among others. Last year, CMU was awarded a $5 million renewal of its National Science Foundation CyberCorps Scholarship for Service program through 2023. We recently launched an undergraduate concentration in security and privacy and expanded our undergraduate course offerings in these areas.

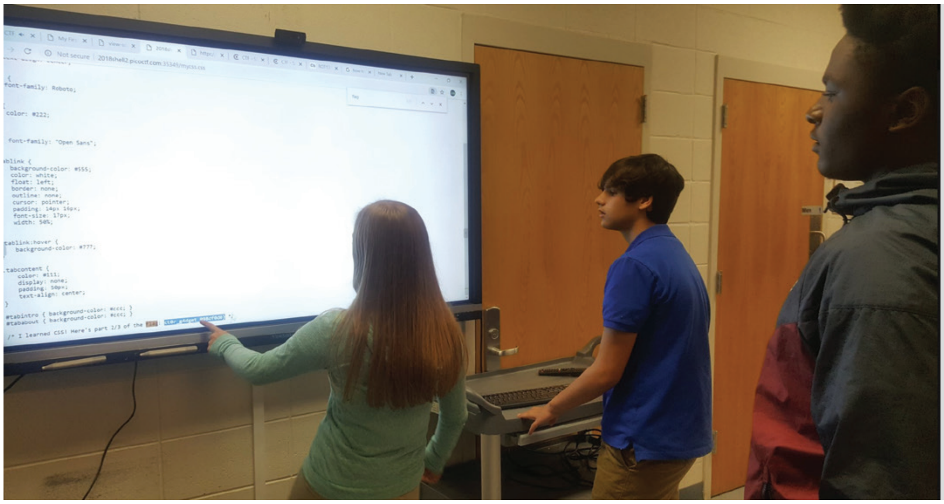
We've had a lot of excitement in the past year. We launched our Secure and Private IoT initiative and funded a dozen projects. Over 27,000 students participated in our picoCTF cybersecurity competition. Professor Virgil Gligor was inducted into the Cybersecurity Hall of Fame, four CyLab faculty won IEEE Cybersecurity awards, and two CyLab researchers won NSA's Best Scientific Cybersecurity Paper Competition. CMU hosted the Women in Cybersecurity (WiCyS) conference in Pittsburgh. A team consisting of researchers from Microsoft Research, Inria, and CyLab released the world's first verifiably secure industrial-strength cryptographic library, "EverCrypt." The Knight Foundation provided $5 million to create The Center for Informed Democracy and Social Cybersecurity (IDeaS) to fight online disinformation. CMU's competitive hacking team, the Plaid Parliament of Pwning, won the "World Cup" of hacking at DefCon for the fifth time in seven years. And I could go on and on!

Please take some time to read more about our accomplishments over the past year as well as in the 15 years since the creation of CyLab. We look forward to continuing collaborations and partnerships over the next 15 years and beyond!

Lorrie Cranor

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

Carnegie Mellon's hacking competition inspires thousands of kids to pursue a career in cybersecurity



Students at Lincoln High School in Lincoln, Alabama, work together to solve a problem in picoCTF 2018.

picoCTF 2019 will be held September 27 - October 11, 2019!

https://picoctf.com

Over 27,000 students participated in the 2018 picoCTF cybersecurity competition, shattering records from previous years. Of the 14,000 US-based student players eligible for prizes, nearly two-thirds of them claimed that they're "more interested in pursuing a career in cybersecurity" as a result of playing picoCTF, according to a post-competition survey.

"Inspiring kids to pursue a career in cybersecurity is the first step in solving the cybersecurity talent shortage," says Marty Carlisle, picoCTF's education lead and a teaching professor in Carnegie Mellon's Information Networking Institute.

A team named "1064CBread," from Dos Pueblos High School in Goleta, CA, is the 2018 picoCTF champion. The team has now won picoCTF a total of four times: every picoCTF competition since the inaugural competition in 2013.

As per tradition, the winning team attended an awards ceremony at Carnegie Mellon.

During a two-week period beginning September 28, thousands of teams around the world attempted to hack, decrypt, reverse-engineer, and do anything necessary to solve 109 computer security challenges created by Carnegie Mellon's internationally-acclaimed hacking team, the Plaid Parliament of Pwning. Anyone could sign up and participate, but only United States students in grades 6-12 were eligible for prizes.

According to a post-competition survey completed by more than 1,000 of the US-based student players, 30 percent of students had no prior experience in hacking and/or cybersecurity. Fifty-seven percent of students said they had "a little bit" of prior experience, meaning nearly 90 percent of students who participated had little to no prior experience in cybersecurity.

"That's really our goal," says Carlisle. "We want to encourage kids who haven't heard of or are relatively new to cybersecurity that this is something they can do – something they might be good at and could potentially build a career out of."

Participants' experiences were very positive, with nearly 90 percent of all survey respondents saying they would recommend playing picoCTF next year.

Shown below are the top 10 winning teams in picoCTF 2018 (teams with the same number of points were ranked according to the time in which those teams gained that many points).

1064CBread - 35,135 pts
Dos Pueblos High School, Goleta, CA

Stallman's Recycle Plant - 34,385 pts
Suncoast Community High School, Riviera Beach, FL
Spring-Forward Senior High School, Royersford, PA
West Windsor-Plainsboro High School North, Plainsboro Township, NJ

ihscyber2 - 32,585 pts
Interlake High School, Bellevue, W

Diesel Locomotive - 32,585 pts
Liberal Arts and Science Academy, Austin, TX

redpwn - 32,485 pts
Scarsdale High School, Scarsdale, NY
Interlake High School, Bellevue, WA
Soundview Prep, Yorktown Heights, NY
Whitefish Bay High School, Whitefish Bay, WI
Homeschool, PA

West - 31,685 pts
Plano West Senior High School, Plano, TX

tjcsc - 31,685 pts
Thomas Jefferson, Alexandria, VA

pearl - 30,835 pts
Montgomery Blair High School, Silver Spring, MD

cppio - 30,835 pts
West Windsor-Plainsboro High School North, Plainsboro Township, NJ

Point Mass - 30,835 pts
Liberal Arts and Science Academy, Austin, TX

As advertised? Exposing lies about VPN locations

One afternoon, roughly two years ago, CyLab postdoc researcher Zack Weinberg noticed something a little odd.

Weinberg was conducting a study about web censorship, using Virtual Private Networks (VPNs) to route web requests from his computer in Pittsburgh through servers located in various countries of interest in order to see what internet users in those countries were able to see online.

"If you're in Saudi Arabia and you try to visit a gambling website, you're supposed to get a screen that says gambling is prohibited in Saudi Arabia," Weinberg says. "But that didn't happen for me, even though the VPN I was using claimed to be in Saudi Arabia."

It turns out the VPN was lying; its servers were actually located in a datacenter in Germany.

This led Weinberg to pursue a whole new study, "How to Catch when Proxies Lie: Verifying the Physical Locations of Network Proxies with Active Geolocation." Weinberg, who recently graduated with a Ph.D. in Electrical and Computer Engineering, presented his findings at ACM Internet Measurement Conference in Boston.

Beyond research purposes, many people use VPNs to circumvent eavesdropping on their internet activity that may occur in their country or to bypass restrictions on content in their country, such as a sporting event that may be "blacked out" in their location. If VPNs lie about their location, users may not get what they want.

Weinberg and his co-authors figured out a way to approximate actual locations of VPNs based on the amount of time it took for a server in the unknown location to send a packet of data to a server in a known location—generally referred to as "ping time."

"It's a similar principle to GPS," Weinberg says. "You ping a server from Pittsburgh, and you learn that it took 20 milliseconds. You do this from a whole bunch of servers with known locations all over the world, draw some circles on a map, and you can see where they all intersect."

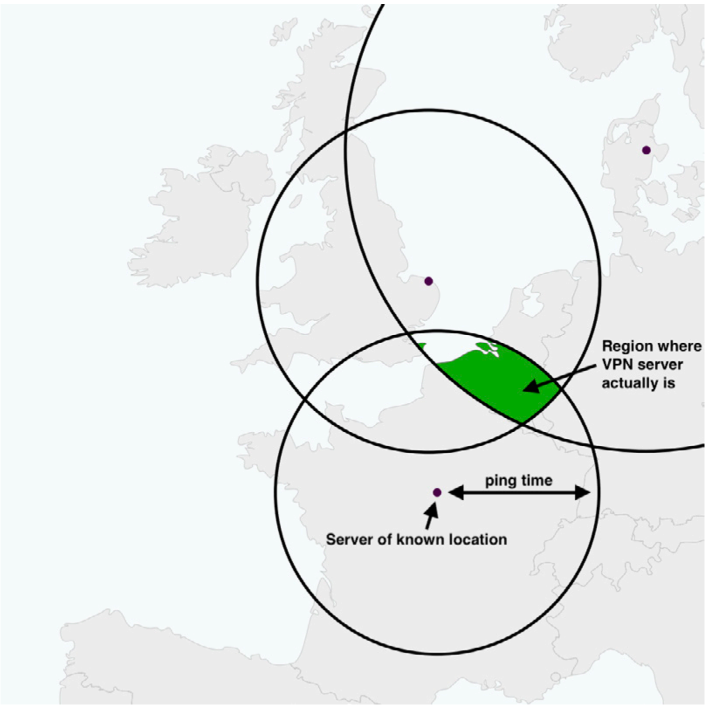
Weinberg and his co-authors estimated the location of 2,269 proxy servers and found that one-third of the servers were "definitely not located in the advertised countries, and another third might not be."

One VPN service in particular claimed to have servers in almost every country in the entire world, including North Korea, and "a bunch of Pacific islands that probably don't even have cables," Weinberg says.

But, why would a VPN service lie about where its servers are? Weinberg says it probably has to do with costs.

"It's definitely cheaper to have many servers in one location than one server in many locations."

Zach Weinberg, Ph.D., Electrical and Computer Engineering



Based on ping times, Weinberg and his co-authors were able to triangulate where a VPN's server may actually be located.

CyLab researchers figured out a way to approximate actual locations of VPN servers based on the amount of time it took for a server in the unknown location to send a packet of data to a server in a known location—generally referred to as "ping time."

"It's definitely cheaper to have many servers in one location than one server in many locations," Weinberg says. "A secondary benefit may be that these VPN providers don't have to do business with a country that is difficult to do business with."

Weinberg says that people using VPNs should be wary about the countries they claim to have servers in.

"If people expect their data is actually going to go through this country and it's not going to go through this other country—if they're genuinely trying to control which jurisdictions their traffic is subject to, which is something that comes up a lot in surveillance—then this is a big concern," he says.

Other authors on the study included Ph.D. student Shinyoung Cho from Stony Brook University, Associate Professor Phillipa Gill from the University of Massachusetts, and CyLab faculty Nicolas Christin and Vyas Sekar.

Virgil Gligor inducted to the Cybersecurity Hall of Fame

CyLab's Virgil Gligor was formally inducted into the Cybersecurity Hall of Fame last April at the Arundel Preserve Hotel in Hanover, Maryland. Gligor was chosen by a senior board based on five criteria: Technology, Policy, Public Awareness, Education, and Business.

"I am thrilled to be given this honor," says Gligor. "Past inductees are true pioneers in the field, and I am humbled to be placed among them."

Since 2008, Gligor has been a professor of Electrical and Computer Engineering, and previously served as the director of CyLab until mid-2015. Throughout his career, he has made fundamental contributions in applied cryptography, distributed systems, and cybersecurity.

Most recently, he authored a breakthrough study on establishing "root of trust," creating a test that – for the first time ever – can detect malware on a device with near certainty.

"Gligor is a pioneer of computer security and has dedicated four decades of his life to exploring cryptography and addressing issues within the cyber world, such as next generation security and trustworthy computing in the face of malware," reads a description of Gligor on the Cybersecurity Hall of Fame website.

After receiving his B.S., M.S. and Ph.D. at the University of California at Berkeley, Gligor taught at the University of Maryland from 1976 to 2007. In 2008, he joined as faculty at CMU and became the second director of the University's CyLab Security and Privacy Institute. He holds an Outstanding Innovation Award from the Association for Computing Machinery, a National Information Systems Security Award from the United States National Security Agency and National Institute of Standards and Technology, and a Technical Achievement Award by the IEEE Computer Society.

The National Cyber Security Hall of Fame was created and supported by companies and organizations committed to recognizing the individuals that played a key role in the creating of the cybersecurity industry.

VIRGIL GLIGOR
CLASS OF 2019
NATIONAL CYBER SECURITY HALL OF FAME
CYBER SECURITY HALL OF FAME

"Past inductees are true pioneers in the field, and I am humbled to be placed among them."

Virgil Gligor, Professor, Electrical and Computer Engineering

CyLab initiatives

Blockchain @ CMU

Blockchains have been touted by technology experts around the world as the next big technological revolution, creating trust where trust never existed before and enabling technologies and services once thought of as science fiction. As part of the Blockchain@CMU initiative, researchers from all across campus are focused on bringing these dreams of blockchain to fruition, focusing their efforts on four main research areas:

- Economics and policy
- Crytopgrahy, security, and anonymity
- Programming languages
- Systems

Cyber Autonomy Research Center

CyLab's Cyber Autonomy Research Center is a university-wide effort focused on research at the intersection of AI and computer security. It seeks to leverage recent transformational advances in machine learning and AI to develop new capabilities to defend our computer systems and networks more effectively and efficiently and minimize human effort. The Center draws on CMU's renowned leadership in AI and in computer security, bringing together faculty from across the University, including the College of Engineering, the School of Computer Science, and the Heinz College of Information Systems and Public Policy.

IoT@CyLab

The Internet of Things (IoT) is reaching critical mass in many sectors of the economy, with the prevalence of IoT devices creating significant challenges for the safety, security, reliability, and privacy of consumers and enterprises that use them. It is increasingly evident that current approaches are ill-equipped to address the security and privacy challenges that will arise in IoT deployments on several dimensions, which IoT@CyLab focuses on tackling:

- Scalability
- Speed and cost
- Safety and security
- Uptime and reliability
- Compliance

IoT@CyLab has been made possible by the generous support of our founding sponsor companies: AT&T, Amazon Web Services, Infineon Technologies, and Nokia Bell Labs.

picoCTF

Recognizing the need to fill the talent gap in the currently struggling cybersecurity workforce, CyLab has created a free, online competition aimed at introducing young minds to the problem-solving skills of cybersecurity. The annual competition, named picoCTF, was first launched in 2013 and has since been played by over 50,000 students from all over the world. During the competition, which typically lasts between one and two weeks, student participants hack, decrypt, reverse-engineer, and do anything necessary to solve computer security challenges created by CyLab's competitive hacking team, the Plaid Parliament of Pwning.

$5M Knight Foundation Investment creates center to fight online disinformation

Kathleen M. Carley, Professor, Institute for Software Research

Bots, trolls, state-run propaganda, information warfare and hate speech are some of the most pervasive ways that societal discourse is being warped in the modern era. In July 2019, Carnegie Mellon University (CMU) announced the creation of a new research center dedicated to the study of online disinformation and its effects on democracy, funded by a $5 million investment from the John S. and James L. Knight Foundation. The new center will bring together researchers from within the institution and across the country.

The Center for Informed Democracy and Social Cybersecurity (IDeaS) will study how disinformation is spread through online channels, such as social media, and address how to counter its effects to preserve and build an informed citizenry. Directed by Kathleen M. Carley, professor in the School of Computer Science's Institute for Software Research, the center will take a multidisciplinary approach, engaging researchers from across the university to examine and develop responses to both technological and human facets of the issue. Douglas Sicker, head of Engineering and Public Policy in the College of Engineering, and David Danks, head of philosophy in the Dietrich College of Humanities and Social Sciences, will be co-directors.

"Addressing the complex issues posed by online disinformation requires robust collaboration from experts spanning sociology and economics, technology and communication theory," said J. Michael McQuade, vice president for research at CMU. "This initiative aligns perfectly with the vibrant collaborative ecosystem we have built at CMU to solve challenges such as these, which are among the most pressing faced by our society. We are thrilled to partner with Knight Foundation on this critical issue."

The center will have three main objectives: expand the body of research across a holistic spectrum of topics, build an interconnected community among the more than 2,000 people working in the field, and educate journalists and policymakers. Its research focus will include topics such as how to better recognize disinformation online, how to identify who is spreading it, how to inoculate groups against it, and how to counter it.

The six-year investment will provide funding for Knight Fellows — graduate students who will deepen their research in related areas. It also will sponsor an annual conference of scientists, practitioners, journalists and policymakers to discuss research and public policy. The investment is part of a broader Knight Foundation initiative that is investing nearly $50 million for research around technology's impact on democracy. The program will provide cross-disciplinary funding to 11 universities and other research and advocacy organizations.

"We are in the middle of a social media war. It's being conducted across Twitter and Facebook, websites, Reddit, pick your favorite media. It is about to get worse with the increased sophistication of bots, memes, and the beginning of deep fakes," Carley said. "Other countries and non-state actors use these tools to impact and shape what you read and who you talk to on social media. The United States doesn't have the tools or the policies it needs to respond. In IDeaS, our goal is to change this."

While the public is exposed to multiple kinds of disinformation, Carley notes the most insidious kind is the one that isn't easily recognizable by the broader public. Examples include innuendos and logical fallacies. These are increasingly spread by large, orchestrated campaigns and disseminated in order to influence group behavior beyond simply absorbing information. For example, in recent elections in many countries including the United States, Sweden, Germany, and the United Kingdom, bots spread disinformation to groups on both sides of contentious issues to polarize them against each other. The result was people in the exposed groups stopped listening to outside information and began operating from an emotional rather than a rational state. This created barriers to communication and understanding between the groups, and in some cases, protests.

> "We are in the middle of a social media war. It's being conducted across Twitter and Facebook, websites, Reddit, pick your favorite media."
>
> *Kathleen M. Carley, Professor, Institute for Software Research*

The center's goal is to develop effective solutions with teams of experts in network analysis, machine learning, and natural language processing to recognize how the information is being spread; sociologists, psychologists, and philosophers to analyze the individual and group response; and public policy researchers to address issues of governance.

"There is clear evidence that, for all the positive potential of the internet, it has made our democracy vulnerable to misinformation and manipulation," said Sam Gill, Knight Foundation vice president for communities and impact. "Solutions will come from deeper understanding. As one of the world's leading centers of technology research, CMU is perfectly positioned to jump into the breach."

IDeaS will build upon the renowned body of multidisciplinary research from CMU's Center for Computational Analysis of Social and Organizational Systems (CASOS), which brings together network analysis, computer science, and organization science; and CyLab, CMU's security and privacy institute.

"This new center is at the heart of what Carnegie Mellon does best as the pioneer of computer science, but also as an institution with a core value of ensuring the effects of technology are positive," said Tom Mitchell, interim dean of the School of Computer Science. "We're uniquely positioned through our deep expertise and strong collaborative culture to create real-world solutions at this critical juncture for society."

CMU crowned hacking champs for fifth time in seven years

Carnegie Mellon University's competitive hacking team, the Plaid Parliament of Pwning (PPP), won its fifth hacking world championship in seven years at this year's DefCon security conference, widely considered the "World Cup" of hacking. The championship, played in the form of a virtual game of "capture the flag," was held August 8-11 in Las Vegas.

PPP now holds two more DefCon titles than any other team in the 23-year history of DefCon hosting the competition.

Three of the five biggest data breaches ever have occurred in the past 12 months, leaking nearly 2 billion personal records. For security experts trying to defend against these types of attacks, the annual DefCon conference provides an opportunity to hone their skills and practice on one another.

"These competitions are so much more than just games," says Zach Wade, a student in Carnegie Mellon's School of Computer Science and one of PPP's team captains. "They bring together the security community to share and test new ideas that can be used to strengthen the security of the systems and devices we use every day."

Over the course of the 72-hour hacking spree, teams made up of students, industry workers, and government contractors attempted to break into each other's systems, stealing virtual "flags" and accumulating points. To add drama, team scores were hidden from view on the second day, and scores and rankings were hidden on the last day, sending teams into a hacking frenzy.

"Our team's success reflects our dedication to training the problem solvers of the future," says Jon Cagan, interim dean of Carnegie Mellon's College of Engineering.

This year's competition consisted of 16 pre-qualified teams with members from at least seven countries around the world. Team "HITCONxBfKin" from Taiwan placed second overall, with team "Tea Deliverers" from China trailing in third.

"This year, we were particularly in the zone for the challenges and our teamwork was very on point," says Carolina Zarate, a recent graduate of CMU's Information Networking Institute. She says the team's camaraderie is an essential aspect of their success, and sums up the 72+ hour experience as involving "(mostly) goofing off, not sleeping, and maybe a little hacking with friends."

The Carnegie Mellon hacking team first formed in 2009 and began competing at DefCon in 2010. The team previously won the contest in 2013, 2014, 2016, and 2017.

> "If you're wondering who the best and brightest security experts in the world are, look no further than the capture the flag room at DefCon."
>
> *David Brumley, Professor, Electrical and Computer Engineering*

PPP stands on stage at DefCon's closing ceremonies as they are announced as winners of the 2019 capture the flag competition.

CMU women shine at Women in Cybersecurity Conference

> "CMU is very focused on the multi-disciplinary nature of cybersecurity."
>
> *Bobbie Stempfley, Director, Software Engineering Institute's CERT Division*

A group of students from CMU's Information Networking Institute pose at WiCyS 2019.

Women make up about one-fifth of the national cybersecurity workforce. That statistic, coupled with Carnegie Mellon University's (CMU's) accelerating number of women working in the field, may help explain why the annual Women in Cybersecurity (WiCyS) conference was hosted by CMU last spring.

"CMU is the birthplace of cybersecurity, and so it's only fitting that we hosted the next-generation of security researchers, hackers and leaders in Pittsburgh," says Dena Haritos Tsamitis, director of CMU's Information Networking Institute (INI).

Haritos Tsamitis joined forces with Bobbie Stempfley, director of the Software Engineering Institute's CERT Division, to help bring the conference to Pittsburgh.

"CMU is very focused on the multi-disciplinary nature of cybersecurity," says Stempfley. "Our partnership in hosting WiCyS enabled us to demonstrate our commitment to advancing all aspects of cybersecurity and highlight an important demographic and their contributions today and in the future."

Coty Gonzalez, a research professor in the department of Social and Decision Sciences, and Dr. Palvi Aggarwal, a postdoctoral fellow in the same department, gave a presentation about the art of deception, and how it's used in attack decisions using cybersecurity scenarios. Gonzalez's expertise on how human behavior affects cybersecurity helped inform a discussion about cognitive models that can be built to represent the process by which attack and defend decisions are made.

CyLab's Coty Gonzalez, a research professor in Social & Decision Sciences, presents at WiCyS 2019.

Lorrie Cranor, director of CyLab, gave a keynote talk about how becoming a computer science professor was, in her words, a "happy accident" that led her to become one of the world's foremost experts on usable security and privacy, a field at the intersection of security, privacy, usability, and human behavior.

Dr. Haritos Tsamitis and Era Vuksani, a Master of Science in Information Security student in the INI, spoke on a panel about the power of women in tech in sparking culture shifts, and various secrets to attracting more women to the cybersecurity field in general. The panel focused on ways to create an equal playing field with equal respect for all.

Ph.D. student Cori Faklaris from the Human-Computer Interaction Institute gave a lightning talk about security interventions for end users. In her talk, Faklaris framed information privacy and security as a public health crisis, which can better help researchers and practitioners approach problems in the usability of security and privacy.

Terri Deasy, assistant director of partnerships in CyLab, helped organize "GenCyber Day" at WiCyS, a full day of presentations and activities attended by nearly 100 local high school students. At GenCyber Day, Megan Kearns, a project manager for CyLab, and Lucia Gonzalez-Prier, Senior Assistant Director of Undergraduate Access and Pipeline Initiatives, presented a variety of different ways for high school students to get involved in cybersecurity, including participating in picoCTF, an online cybersecurity game developed and hosted by CMU.

Also among the conference attendees were INI faculty and security and privacy researchers Aleecia McDonald and Hanan Hibshi.

Security and privacy need to be easy

Back in 2005, Carnegie Mellon University (CMU) hosted a first-of-its-kind conference that brought together researchers from dozens of universities and companies around the world with one mission: make privacy and security tools easier to use.

That conference, the Symposium On Usable Privacy and Security (SOUPS), held its 15th annual meeting in August. SOUPS, as well as the entire usable privacy and security field, have deep roots at CMU.

The early years at CMU

In 1999, one of the first widely read usable security papers, "Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0," was written by a CMU computer science Ph.D. student, Alma Whitten. The paper argued that effective security requires ease in usability, and that most security failures were caused by user errors stemming from clumsy and confusing user interfaces.

In the early 2000s, Lorrie Cranor, who now serves as CyLab's director, grew concerned about usability issues related to a privacy standard she was working on. She looked for research on usable privacy tools that could inform the standards work, and came up empty handed.

"I realized that not a lot was known about how to make privacy or security tools usable," says Cranor. "So, I decided to make that the focus of my research."

Cranor joined CMU's faculty in 2003 and was a key player in building momentum around the field of usable privacy and security. She formed the CyLab Usable Privacy and Security (CUPS) Laboratory in 2004 and started working with students interested in this area.

In 2005, Cranor co-edited the first book on usable privacy and security, and in 2006, she and two other CUPS Lab faculty introduced the first usable privacy and security course at CMU, which is still taught today.

The CUPS Lab

Since its formation, the CUPS Lab has served as an epicenter in the usable privacy and security world. The group, which started out with Cranor accompanied by a modest number of students, now consists of about three dozen faculty and students and has published upwards of 200 research papers in the field.

"One of the ways that usable privacy and security research often differs from other human-computer interaction research is the need to study user behavior in the presence of risk or adversaries," Cranor says.

As a result, CUPS Lab studies often use deception to study how users react to security prompts, without revealing the true purpose of the study. For example, researchers may recruit users to test online video games, but in reality, they are studying users' reactions to pop-up security warnings that the researchers trigger on gaming websites.

One of the earliest CUPS Lab projects resulted in the development of anti-phishing tools, including an interactive game and other security awareness tools. Cranor, Institute for Software Research Professor Norman Sadeh, and Human Computer Interaction Institute Professor Jason Hong, co-founded Wombat Security Technologies to commercialize these tools.

To help people make better decisions about their privacy, Cranor and her students developed a prototype "nutrition label" for privacy in 2009, with the goal of making the privacy policy of a product or service easy to understand and compare with other policies. Now CUPS faculty and students are developing a privacy and security nutrition label for IoT devices.

Sadeh is leading an effort to better inform users' privacy decisions through the development of personalized "privacy assistants" that can advise users about privacy policies and make privacy decisions on users' behalf. Along a similar theme, Sadeh's Usable Privacy Policy Project looks to extract information from privacy policies and display it in useful ways for users.

Lorrie Cranor poses with CUPS Lab students in 2007.

The group has been very influential in passwords research, publishing more than 20 research papers about passwords and developing a data-driven password meter that tells users in real-time how they could make their passwords more secure. Electrical and Computer Engineering and Institute for Software Research (ISR) Professor Lujo Bauer as well as ISR and Engineering and Public Policy Professor Nicolas Christin play key roles in this effort.

Understanding people's behaviors with tools is typically the starting point in trying to understand how to make a piece of technology more usable, and the CUPS Lab does that through its Security Behavior Observatory (SBO), which aims to understand the everyday security and privacy challenges people face using their home computers. Consenting participants in the SBO install software that tracks their computer's activities so researchers can better understand how users interact with privacy and security tools, and what types of online behaviors put users at risk.

Where the field is going

While the field has made leaps and bounds in advancing the vision of making privacy and security tools more usable, there is still much to be accomplished. (News to no one: privacy policies are still unreadable). Part of that comes down to the field improving its research methods.

"Usable privacy and security research is becoming more rigorous and reproducible," says Cranor. "Going forward I expect to see more generalizable principles coming out of this work."

Cranor also expects to see more exploration of usable privacy and security issues related to emerging technologies, as well as use of machine learning techniques to personalize privacy and security tools for users.

CyLab Distinguished Seminar Series

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

Lea Kissner, Chief Privacy Officer at Humu, presents at the CyLab Distinguished Seminar Series.

Vinod Vaikuntanathan
Associate Professor of Electrical Engineering and Computer Science at MIT

Problems in Information-Theoretic Cryptography

Michael Bailey
Associate Professor at the University of Illinois at Urbana-Champaign

This is Why We Can't Have Nice Things: Cautionary Tales from Empirical Systems Security Research

Frank Greitzer
Principal Scientist and founder of PsyberAnalytix

Sum of All Fears: Status of Two Decades of Modeling Insider Threat Risk

Jonathan Aldrich
Professor of Computer Science at CMU

Usable Architecture-Based Security in the Wyvern Language

Richard Linger
CTO of Lenvio, Inc.

Crossing a Chasm: The Journey from Lab Prototype to Commercial Product

Art Brock
Founder of Holochain

Think Outside the Blocks: Taking Apps Mainstream with Holo and Holochain

David Kotz
Interim Provost and Champion International Professor in the Department of Computer Science at Dartmouth College

Secure, Intentional Communications with Mobile Devices

Sam Weber
CyLab Senior Systems Scientist

Empirical Security Engineering

Scott Ruoti
Electrical Engineering & Computer Science Professor at the University of Tennessee

Understanding Blockchain Technology and Its Use Cases

Gireeja Ranade
Assistant teaching professor at UC Berkeley

"Fake news," Russian propaganda, and elections

Harsh Patil
Sr. Staff Research Engineer at LG Electronics Mobile Research

Security and privacy for the connected vehicle technology

Giulia Fanti
Professor of Electrical and Computer Engineering at CMU

Compounding of Wealth in Proof-of-Stake Cryptocurrencies

David Lazar
Ph.D. student at MIT's Computer Science and Artificial Intelligence Lab

Karaoke: Distributed Private Messaging Immune to Passive Traffic Analysis

Rafail Ostrovsky
Professor of Computer Science and Mathematics at UCLA

Towards Stronger Cloud Security

Lea Kissner
Chief Privacy Officer at Humu

Building for Trust: Because we don't all have to learn privacy lessons the hard way

Weidong Cui
Principle Researcher at Microsoft Research

Triaging and Debugging Failures in Deployed Software by Reverse Execution

Kevin Werbach
Professor at the Wharton School, University of Pennsylvania

The Blockchain as a New Architecture of Trust

Nancy Mead
Fellow and principle researcher at the Software Engineering Institute

Threat Modeling Research and Machine Learning

Suraj Kothari
Professor of Electrical and Computer Engineering at Iowa State University

An 18th-century Mathematician, a $336 Million Patent, and Software Verifiability

Eunsuk Kang
Assistant professor in CMU's Institute for Software Research

Model-Driven Security: Challenges and Applications

Security and Privacy Degree Programs Offered at CMU

Across the colleges and schools at Carnegie Mellon, a number of professional graduate degree programs are offered in security and privacy.

Undergraduate Concentration in Security & Privacy

This past year, CMU launched a new Security & Privacy concentration for undergraduate students designed to expose students to the key facets of and concerns about computer security and privacy that drive practice, research, and legislation. Upon 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 offers a technical focus in security and computer systems, which is 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 Pittsburgh-Silicon Valley Master of Science in Information Technology offers two degrees through bicoastal delivery in collaboration with CMU's Silicon Valley campus: Mobility (MSIT-MOB) and Information Security (MSIT-IS).
- The Master of Science in Information Technology - Privacy Engineering (MSIT-PE) degree is a one-year 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 Networking (MSIN) degree provides an advanced, specialized curriculum combining computer science, electrical and computer engineering, software engineering, and information systems while incorporating business and policy perspectives.
- The Master of Science in Information Security Policy and Management (MSISPM) 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.
- Students in the Master of Science in Electrical and Computer Engineering (MS-ECE) program are provided with a thorough background in the fundamentals of electrical or computer engineering, as well as the opportunity for in-depth specialization in some particular aspect of these fields, such as security and privacy.

Ph.D. Programs

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

- Ph.D. Programs at the School of Computer Science include Human-Computer Interaction, Machine Learning, Software Engineering, Computer Science, and Societal Computing.
- Ph.D. programs in the College of Engineering include Electrical and Computer Engineering (ECE) and Engineering and Public Policy (EPP).

CyLab Executive Education Offerings

Over the past year, CyLab has been collaborating with CMU's Tepper School of Business to develop exciting executive education opportunities related to security and privacy.

CyLab also provides custom executive education programs that are developed to meet the needs of an organization.

Blockchain Executive Education Programs

Leveraging blockchain requires understanding how the technology can be integrated with business, and that's exactly why CyLab and the Tepper School of Business have developed a Blockchain Executive Education Program. The program works with leaders at all levels to translate the emerging research from CMU's blockchain research thrusts to actionable business value.

Internet of Things (IoT) Cybersecurity Executive Education Programs

As IoT cybersecurity is reaching critical mass in many sectors of the economy, CyLab and the Tepper School of Business are developing executive education that delivers programs to assess emerging IoT technologies and current use cases, and translate these into opportunities to create innovative product and service offerings, increase operational efficiencies, reduce risk, and collaborate with ecosystem partners. Set to launch in the Spring semester of 2020, the programs will provide a baseline of foundational knowledge, updates on new developments, and engagement on the potential for business impact.

Interested in learning more about these executive education offerings?
Email partnerships@cylab.cmu.edu to learn more.

CyLab Core Faculty

CyLab's faculty bring security and privacy expertise from across the University.

Alessandro Acquisti
Professor, Heinz College

Yuvraj Agarwal
Assistant 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

Jason Hong
Professor, Human-Computer Interaction Institute

Limin Jia
Associate research professor, ECE, INI

Timothy Libert
Special faculty instructor, ISR

Radu Marculescu
Kavçiç-Moura professor, ECE

Piotr Mardziel
Systems scientist, ECE

Aleecia McDonald
Assistant professor of the practice, INI

Bryan Parno
Associate professor, CSD, ECE

Corina Pasareanu
Associate research professor, 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
Associate professor, ECE

Douglas Sicker
Professor, EPP, ISR

Asim Smailagic
Research professor, Engineering Research Accelerator

Patrick Tague
Associate research professor, ECE; Associate director, INI

Conrad Tucker
Professor, Mechanical Engineering

Sam Weber
Senior systems scientist, CyLab

Maverick Woo
Systems scientist, CyLab

Osman Yagan
Associate research professor, ECE

Featured Speaking En

Alessandro Acquisti

"Privacy, Behavior, and Economics"
Keynote Talk: University of Bologna Business School, Marketing Effectiveness through Customer Journeys and Multichannel Management Conference, Bologna,
June 2019

"Shaping Competition Policy in the Era of Digitisation"
Panelist at the European Commission, Brussels, January 2019

"Hearing on Privacy, Big Data, and Competition"
Panelist at the Federal Trade Commission, Washington DC, November 2018

"Privacy, Economics, and Regulation: A Note"
Invited talk, Atlanta FED, 24th Financial Markets Conference, May 2019

Lujo Bauer

"IoT, privacy, and machine learning: (Avoiding) some challenges and pitfalls"
CERT Data Science in Cybersecurity Symposium, Arlington, VA, Aug. 29, 2018

"Physically realizable attacks on ML + Measuring password strength with DNNs"
Google Security & Privacy Research Awards Workshop, Oct. 29, 2018

"Attacking AI-based face recognition + Detecting code injection on the web"
Counter-cybercrime Technology and Investigation Symposium, Tokyo, Japan, Dec. 5, 2018

"Machine learning in the presence of an attacker"
IARPA Emerging Threats Seminar, Aspen Institute, Washington DC, Apr. 2, 2019

Kathleen Carley

"Social Cyber-Security Dynamics"
Keynote Computational Social Science – Quo Vadis? An Interdisciplinary Symposium Honoring Kathleen M. Carley, University of Zurich, Zurich Switzerland, April 2019

"Information Maneuver Assessment"
Keynote StratComAPAC2019, Singapore, April 2019

ngagements

"Social Cyber-Security"
Keynote IEEE Intelligence and Security Informatics, Florida International University, Miami, FL, November 2018

"Social Cyber-Security"
Keynote MOBICOM, Delhi, India, October 2018

Martin Carlisle

"Using picoCTF to Teach Introductory Computer Security Concepts"
Presented workshop at Computer Science Teachers Association Conference, Phoenix AZ, July 7, 2019

Lorrie Cranor

"Tales of an Accidental Computer Science Professor"
Keynote talk at the Women in Cybersecurity 2019 (WiCys), Pittsburgh, PA, March 29, 2019

"Security and Privacy for Humans"
Keynote talk at Expeditions in Computing: 10 years transforming science and society, Washington, DC, December 6, 2018

"Consumer Demand and Expectations for Privacy," FTC Hearing the FTC's Approach to Consumer Privacy, April 9, 2019

"Designing Notice and Consent for the Internet of Things," International Association of Privacy Professionals Global Privacy Summit 2019, Washington, DC, May 1, 2019.

Lorrie Cranor co-chaired the first USENIX Conference on Privacy Engineering Practice and Respect (PEPR'19) in August with CyLab Alumna Lea Kissner.

Dena Haritos Tsamitis

"Fraud Alert: Shatter Impostor Syndrome"
The Diana Initiative Speaker, August 2018

"Changing the Diversity Game, One Scholarship Recipient at a Time"
International Consortium of Minority Cybersecurity Professionals (ICMCP) Speaker, September 2018

"Fraud Alert: Shatter Impostor Syndrome"
Grace Hopper Celebration of Women in Computing (GHC) Speaker, September 2018

Norman Sadeh (far left) served on a plenary panel on privacy and ethics at the International Conference of Data Protection and Privacy Commissioners (ICDPPC) in Brussels.

"Paying it Forward: How Women in Tech Groups Can Spark a Culture Shift, and How You Can Help!"
Women in Cybersecurity (WiCyS) Panel Moderator, March 2019

Jason Hong

"Security and Privacy Challenges for IoT Security, Privacy and Human Behavior"
RSA Conference, Mar 4, 2019

"How We Will Fail in Privacy and Ethics for the Emerging Internet of Things"
UCSD HDSI Mini Symposium on Security + Privacy, February 28, 2019.

"Are My Devices Spying On Me? Living in an Age of Ubiquitous Computing."
Lakehead University, "Rise of the Machines", February 26, 2019

"Helping Developers with Privacy"
Keynote Speaker at the IEEE Symposium on Visual Language and Human-Centric Computing Oct 2, 2018

Corina Pasareanu

"Symbolic Execution and Probabilistic Reasoning"
Invited talk at the 16th International Symposium on Automated Technology for Verification and Analysis, Los Angeles CA., October 2018

Bryan Parno

"Provably Secure, Provably Isolated Code"
DARPA ISAT Principled Hardware/Software Interfaces (PHI) Workshop, February, 2019.

Jon Peha

"How Multi-Network Access Agreements among Cellular Operators and MVNOs Could Reduce Cost"
Keynote talk at the 18th IEEE Wireless Telecommunications Symposium, New York City, April 2019

Norman Sadeh

"MAPS: Scaling Privacy Compliance Analysis to a Million Apps"
Privacy Enhancing Technologies Symposium, July 2019

"Our Privacy Infrastructure for IoT and our work on Personalized Privacy Assistant"
IAPP Global Privacy Summit, May 2019

"Wombat Security Technologies: How We Got to a $225M Exit by Phishing our Customers"
TiE Pittsburgh keynote, Schwartz Center for Entrepreneurship, Carnegie Mellon University, November 29, 2018

"Debating Ethics: Dignity and Respect in Data-Driven Life"
Panelist, 40th International Conference of Data Protection and Privacy Commissioners, European Parliament, Brussels, October 2018

Featured Grants Received by Faculty

Lujo Bauer, Matt Fredrikson, and **Mike Reiter** were awarded an NSF grant for their project, *"Using Machine Learning to Build More Resilient and Transparent Computer Systems."*

Jan Hoffman was awarded the *Faculty Early Career Development (CAREER) Award*, the National Science Foundation's most prestigious award for young faculty members. The NSF award will support his work regarding quantitative properties, such as available memory and execution time, associated with formal verification techniques.

Dena Haritos Tsamitis was awarded a $5 million renewal of the *CyberCorps® Scholarship for Service (SFS) Program* through 2023. The SFS@CMU program provides students a full-tuition scholarship and a generous stipend for living expenses in exchange for government service in a cybersecurity role after graduation.

Corina Pasareanu and collaborators from UC-Berkeley and UC-Santa Barbara were awarded an NSF grant for *"HUGS: Human-Guided Software Testing and Analysis for Scalable Bug Detection and Repair."*

Kathleen Carley, Doug Sicker, and **David Danks** were awarded a $5 million grant for the Knight Foundation to create the *Center for Informed Democracy and Social Cyber-Security (IDeaS).*

Osman Yagan was awarded an NSF grant for his project, *"Contagion Processes in Multi-layer and Multiplex Networks."*

Fei Feng was awarded a grant from the U.S. Army Combat Capabilities Development Command's Army Research Laboratory for a project titled, *"Learn to Defend Against Unknown Attackers and Deceptive Attacks."*

Norman Sadeh was awarded a $1.2 million grant from the NSF to develop and evaluate a privacy assistant to answer people's privacy questions.

Norman Sadeh was awarded an NSF grant to inform the development of privacy controls in mobile and IoT applications using contextual integrity.

Featured Faculty Recognitions

2018 IEEE Cybersecurity Award for Practice
Recipient: Lujo Bauer, Nicolas Christin, Lorrie Cranor, and collaborators, in recognition of their body of research on password security.

2018 IEEE Cybersecurity Award for Innovation
Recipient: Alessandro Acquisti, for his groundbreaking work on the economics and behavioral economics of privacy and personal information security.

SC Magazine's 2018 Women in IT Security Power Player
Recipient: Dena Haritos Tsamitis, for her achievements in information security and education.

Best Paper Award at ACM MobiHoc 2019
Recipient: Giulia Fanti and collaborators, for their paper, "Barracuda: The Power of ℓ-polling in Proof-of-Stake Blockchains."

Honorary Doctorate, Faculty of Business, Economics and Informatics at University of Zurich
Recipient: Kathleen Carley, for "pioneering contributions to our understanding of social systems by means of computational methods. Through the development of new methods to study social networks, she shaped the development of data science and computational social science and provided important stimuli for the study of digital societies."

Most Influential Paper Award at Automated Software Engineering 2018
Recipient: Corina Pasareanu and collaborators, for their paper, "Assumption Generation for Software Component Verification," originally presented at ASE 2002.

2019 Class of Andrew Carnegie Fellows by the Carnegie Corporation of New York
Recipient: Lorrie Cranor

Test of Time award at the 2018 ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering
Recipient: Corina Pasareanu and collaborators for their paper, "Differential Symbolic Execution," originally presented in 2008.

Retrospective Impact Award at the 2018 International Symposium on Software Testing and Analysis
Recipient: Corina Pasareanu and collaborators for their paper, "Test Input Generation with Java Pathfinder," originally published in 2004.

Board of Directors appointee for RSA Conference (2018-present)
Recipient: Dena Haritos Tsamitis

Board of Advisors appointee for Minorities in Cybersecurity (2018-present)
Recipient: Dena Haritos Tsamitis

NSA's Best Scientific Cybersecurity Paper Award
Recipients: Tiffany Bao and David Brumley

CyLab's 2019 Presidential Fellows

Each year, CyLab awards Presidential Fellowships to high-achieving exemplary graduate students researching topics around security and privacy. Each fellowship covers one year of tuition.

This year's Fellows were selected by a committee of CyLab faculty, including Nicolas Christin, Yuvraj Agarwal, Virgil Gligor, Radu Marculescu, and Corina Pasareanu. Committee members did not participate in the evaluation of any of their own students who were nominated.

This year's CyLab Presidential Fellowship recipients are:

Aymeric Fromherz, Ph.D. student in Electrical and Computer Engineering (ECE)

Co-advised by ECE professor Bryan Parno and CyLab research professor Corina Pasareanu

Fromherz's research focuses on designing and focusing secure-by-construction systems. Most of his recent work is about providing formal security guarantees for highly efficient implementations of cryptographic primitives and protocols.

"Machine learning algorithms increasingly permeate our environment. With this fellowship's support, I hope to apply my expertise in formal methods to defend against attacks against neural networks."

Pardis Emami-Naeini, Ph.D. student in the Institute for Software Research (ISR)

Co-advised by Engineering and Public Policy / ISR professor Lorrie Cranor and ISR / Computer Science Department (CSD) professor Yuvraj Agarwal

Emami-Naeini's research focuses on creating tools and methods that enable people to make better security and privacy decisions in the world of the Internet of Things (IoT).

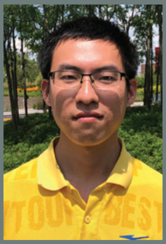
"Large-scale user studies are expensive to conduct properly, but the CyLab Presidential Fellowship will provide me with more freedom to conduct projects I was envisioning in order to design a usable and effective privacy and security label for IoT devices."

Hana Habib, Ph.D. student in Societal Computing

Advised by EPP / ISR professor Lorrie Cranor

Habib's research explores the usability of consumer privacy choices, such as opt-outs for email marketing and targeted advertising. She hopes to identify usability barriers with existing privacy choices and solutions to mitigate them so that consumers can ultimately have greater control over their privacy.

"This fellowship will allow me to make a meaningful contribution to privacy research through fulfilling a need for a validated set of concrete design guidelines that companies and regulators can refer to for providing meaningful privacy choices to users."



Yifan Song, Ph.D. student in the CSD

Advised by CSD professor Vipul Goyal

Song's research aims to construct a communication-efficient multi-party computation (MPC) protocol, which allows several parties who do not trust each other to securely compute a function.

"I feel very honored to be selected as one of the CyLab Presidential Fellows. This funding will greatly support my research on designing communication-efficient MPC protocols."

Graduated Ph.D. Students

Jassim Aljuraidan, Ph.D. in ECE
Advisor: Lujo Bauer
Thesis title: Information-Flow Control in Modern App Platforms: Modeling, Formal Verification, and Controlled Declassification *Defense:* December 2018
Current position: Assistant Professor, Kuwait University

Rashad Eletreby, Ph.D. in ECE
Advisor: Osman Yagan
Thesis title: New Models for the Structure of and Spreading Processes in Complex Networks
Defense: September 2019
Next destination: Walmart Labs

Alexandre Ligo, Ph.D. in EPP
Advisor: Jon Peha
Thesis title: Connected Vehicles for Internet Access: Deployment and Spectrum Policies
Defense: December 2018

Abigail Marsh, Ph.D. in Societal Computing
Advisor: Lorrie Cranor
Thesis title: An Examination of Parenting Strategies for Children's Online Safety
Defense: August 2018
Current position: Assistant professor of computer science at Macalester College

Steve Matsumoto, Ph.D. in ECE
Advisor: Bryan Parno
Thesis title: Effective and Practical Improvements to the Web Public-Key Infrastructure
Defense: February 2019
Current position: Assistant Professor at Olin College

William Melicher, Ph.D. in ECE
Advisor: Lujo Bauer
Thesis title: Modeling Security Weaknesses to Enable Practical Run-time Defenses
Defense: May 2019
Current position: Staff security researcher, Palo Alto Networks.

Yingrui Zhang, Ph.D. in ECE *Advisor:* Osman Yagan
Thesis title: Modeling, Analysis, and Optimization of Robustness in Interdependent Networks against Cascading Failures
Defense: May 2019

Yong Zhuang, Ph.D. in ECE *Advisor:* Osman Yagan
Thesis title: Information and Influence Propagation in Multi-layer Networks: the Impact of Clustering, Multi-dimensional Content Spreading, and Information Mutation
Defense: September 2019

Featured CyLab Media Mentions

WIRED

CyLab's Vipul Goyal comments on HTC's new "blockchain phone"

OCTOBER 23, 2018

WIRED interviewed CyLab's Vipul Goyal about HTC's new "blockchain phone," which, though a commerical product, acts more as an experimental prototype to explore the future of blockchain technology on phone security. "A private key protected by special hardware architecture and OS interface can be far more secure than one stored by a wallet app downloaded from an app store," said Goyal, who also added that another advantage of blockchain phones is battery efficiency.

Chicago Tribune

McDonald interviewed about California's new privacy law

SEPTEMBER 25, 2018

The *Chicago Tribune* interviewed CMU-SV's Aleecia McDonald about California's new internet privacy law. McDonald says, "Consumers will…have the right to know when their personal information is being sold to a third party…and to opt out of that sale." She thinks it is "entirely plausible" that other states will adopt a similar law and consumers everywhere might start to see buttons on sites allowing them to opt out of their personal data being sold.

QUARTZ

Mozilla uses CyLab tool for cybersecurity shopping guide

NOVEMBER 15, 2018

A recent IoT device shopping guide created by the Mozilla Foundation revealed that only a small number of the devices actually met recommended security standards. The guide also used an algorithm created by CyLab's Usable Privacy Policy Project to assess the reading levels necessary to comprehend various privacy policies. Mozilla found that the average privacy policy was written at a college reading level, which experts identified as a major transparency concern.

Christin says dark-web ecosystem undented by law enforcement efforts

MAY 9, 2019

Despite having brought down multiple marketplaces for illicit goods and drugs over the past several years, law enforcement officials across the world are still struggling to contain the emergence of new dark-web markets to replace them. "History has taught us that this ecosystem is very, very resilient," says CyLab's Nicolas Christin "It's part of a cycle, and we're in the chaotic part of the cycle. We'll have to see how it recovers. But if I were a betting person I would put more money on it recovering than on it dramatically changing." International law enforcement has made major improvements in coordination and methodology, but according to Christin, their efforts don't "seem to have dented the ecosystem in a major way."

The New York Times

CyLab researchers quoted in NYT

NOVEMBER 14, 2018

CyLab's Marios Savvides, Lujo Bauer, Jason Hong, Kathleen Carley, Martin Carlisle, and Carolina Zarate were featured in a *New York Times* piece about various ongoing research thrusts in CyLab to help combat cyberattacks. "More than 300 researchers and graduate students are working or studying at CyLab this year, making it among the largest cybersecurity training centers in the world," the article says.

Libert found Facebook and Google trackers on porn sites

JULY 17, 2019

A new study conducted by CyLab's Tim Libert and other researchers has scanned 22,484 pornography sites and found them riddled with trackers from major technology companies such as Facebook and Google. 93% of these websites sent data to an average of seven third-party domains, and only 17% of them have privacy policies. Facebook and Google denied that they used information collected by their trackers on pornography websites for creating marketing profiles, but it is unclear why they are collecting data from those websites.

The Washington Post

Brumley comments on offensive cyber operations

FEBRUARY 11, 2019

ECE/CyLab's David Brumley was interviewed by the *The Washington Post* about the Trump administration's goal for loosening constraints on offensive cyber operations. A majority of security experts agree with the move, which allows the U.S. to challenge international adversaries and reconsider their attacks, but they advise to proceed carefully and caution against giving the military free reign. Brumley believes the move is "common sense" on an operational level. "The military should be able to use their judgment—within the confines of law—to determine where and how to conduct an offensive cyber operation," he said. "Allowing the men and women who are experts in cyber to make the call on how to use cyber is common sense."

KQED

Rajkumar comments on the future of autonomous cars

FEBRUARY 9, 2019

ECE’s Raj Rajkumar was quoted in an article by KQED that discusses why autonomous cars have a long way to go before they become mainstream and available across the country. While ample research and development are occurring in Pittsburgh and Silicon Valley for companies like Uber and Google’s Waymo, there are several reasons why the industry needs at least 10 years—probably more—of technological development. One reason is the weather, particularly snow, that is hard to predict and even harder to control. Heavy snow, rain, fog, and other conditions obstruct the view of the cars’ cameras, interfering with object recognition sensors. “It’ s like losing part of your vision,” Rajkumar said.

NBC NEWS

Sekar comments on automated visitor security systems

MARCH 18, 2019

ECE/CyLab’s Vyas Sekar was interviewed by NBC News about the safety and privacy of automated visitor security systems, which are replacing receptionists and security guards in businesses, schools, hotels, and hospitals. An IBM X-Force Red study revealed that five different systems are vulnerable in previously unknown places, making not only individuals’ information susceptible, but also company information if connected to a wider network. “An attacker always looks for the weakest link, so if they find one of these systems that collects personal data and is network-connected, it’s like a goldmine for them,” Sekar said. “If these systems are not secured and a company does not have the right security practices in place, then that’s a big security risk.”

POPULAR SCIENCE

Rowe discusses FCC’s proposed plans to quicken Wi-Fi

OCTOBER 25, 2018

The Federal Communications Commission (FCC) has announced potential plans to make a new part of the wireless spectrum available to Wi-Fi devices. According to ECE’s Anthony Rowe, this change—which would allow devices to access the 6 gigahertz (GHz) region in addition to the 2.4 and 5 GHz regions already available—would provide faster Wi-Fi, nearly tripling the available bandwidth. If pursued, this plan would ultimately quicken download and upload speeds, especially for users in crowded public places where everyone is trying to use the same network.

Parno quoted in PopSci on end-to-end encryption

MARCH 8, 2019

Mark Zuckerberg’s recent announcement regarding end-to-end encryption and the future of Facebook’s messaging services has stirred up quite a bit of chatter within the tech communities. While encryption is essential to privacy, leading experts in the field point out that there are both pros and cons. One proponent of encryption is ECE’s Bryan Parno, who emphasizes that it is essentially impossible to break. “To the best of our knowledge, as cryptographers, the amount of time it would take to decrypt those messages without knowing the key is hideously large,” Parno told *Popular Science.*

THE WALL STREET JOURNAL.

Acquisti quoted on possible impacts of stricter data privacy rules

JANUARY 21, 2019

CyLab’s Alessandro Acquisti was quoted in a *WSJ* article about how big tech companies like Facebook and Google handle customers’ personal information and what stricter privacy rules could do to these companies. Some say that stricter rules will benefit big companies that have more resources at their disposal, but others say that stricter rules will undercut big companies’ advertising and weaken their advantage over smaller companies. Acquisti says, “Both are reasonable claims. But it is far too early to tell which will turn out to be true.”

c|net

Cranor says Facebook views user data as “a corporate asset”

DECEMBER 5, 2018

CyLab/EPP’s Lorrie Cranor recently commented for *CNET* in the wake of troubling emails that have emerged regarding data privacy practices at Facebook. While public concern has repeatedly been raised after multiple data privacy incidents at the company over the last couple years, the emails appear to cast doubt on Facebook’s claims that it does not sell user data. “This email certainly doesn’t express any value of privacy or protecting users,” says Cranor. “This is expressing that data is a corporate asset, and that we don’t want to give it away.”

Savvides comments on AI and facial recognition

MARCH 28, 2019

CyLab/ECE’s Marios Savvides spoke with CNET in an article about how AI has helped to drastically improve facial recognition. While there are privacy and bias concerns, facial recognition is now being used more widely, at airports, in home security systems, and on cruises, with a 99.7 percent accuracy for the most cutting-edge systems. However, even deep learning neural networks can make mistakes. Savvides, director of the CyLab Biometrics Center, separates some of the data to make things clearer for the neural net. His team can reconstruct faces even in conditions that aren’t optimal. “We live in a time where AI can surpass the human brain’s capability,” he says.

Featured CyLab Events

Jingyi "Amanda" Zhu (left) and Kentrell Owens (right) talk about privacy at CMU's International Data Privacy Day celebration.

Army War College visits CyLab

Members of the United States Army War College International Fellows Program visited Carnegie Mellon for a day of talks given by CyLab faculty on the latest security and privacy research. Each year, tens of senior military officers from as many different countries are extended an invitation from the Chief of Staff of the United States Army to attend the U.S. Army War College. The academic year is full of studying, research, and fellowship as these officers are exposed to and instructed in areas ranging from military concepts and doctrine to national and theater level strategies.

Women in Cybersecurity Conference

Around 1,000 women in the cybersecurity field from around the nation, from those in senior roles to the next wave of female technologists, met in Pittsburgh this past year as Carnegie Mellon University hosted this annual Women in CyberSecurity (WiCyS) conference. CMU faculty, students, and alumni were among the keynote speakers and panelists. The WiCyS Conference annually attracts students, professionals and leaders in the cybersecurity field. Half of the participants are students attending through scholarships awarded by WiCyS with the support of its sponsors.

International Data Privacy Day

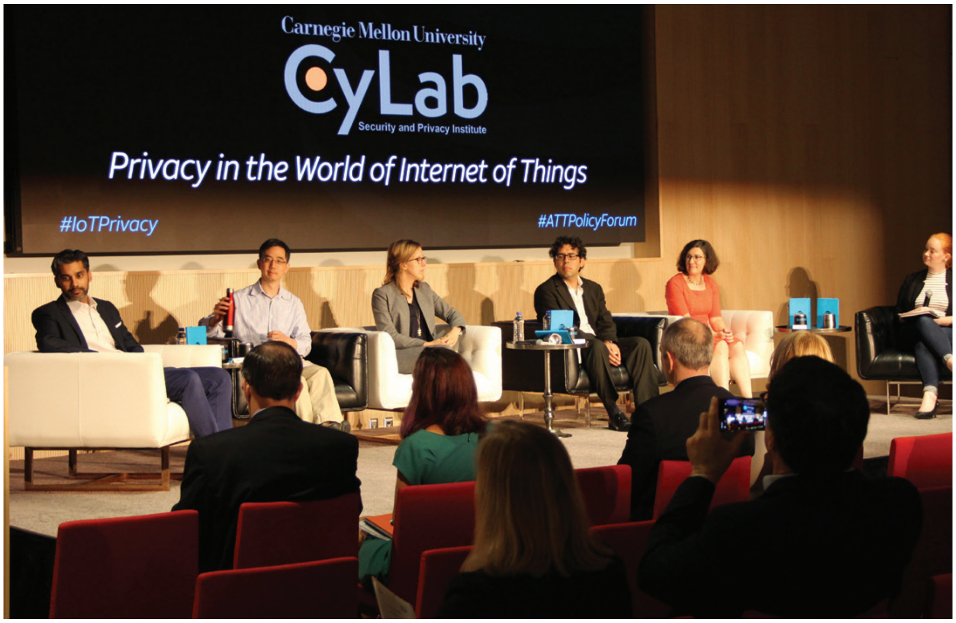
Carnegie Mellon celebrated International Data Privacy day by presenting privacy research and practical advice on protecting privacy online. During the event, a privacy clinic was held where students in CMU's Privacy Engineering Master's program took questions from attendees about how they could better protect their digital privacy. Students also held a research poster session where they presented their latest privacy research.

19th USSOCOM Sovereign Challenge Conference

The United States Special Operations Command (USSOCOM) partnered with CMU to host the 19th Sovereign Challenge Conference. The theme of this year's conference, "Technological Change and Its Effect on Future of Irregular Warfare," was discussed and debated by professors and influencers who are acknowledged experts in the field. This included discussions about the efficacy and ethics of using machine learning and artificial intelligence on the battlefield, especially the determination of responsibility when something goes wrong with the technology. The conference included more than 120 representatives from around the world.

AT&T Policy Forum: Privacy in the World of Internet of Things

Carnegie Mellon University hosted the AT&T Policy Forum, one of several policy forums run by AT&T to discuss various aspects of emerging technologies. This policy forum focused on one of the most challenging issues consumers and businesses face in a world of smartphones, wearables and other internet-connected devices: privacy. The event included a privacy panel consisting of privacy experts, including CyLab faculty.


Carnegie Mellon University
CyLab
Security and Privacy Institute
Privacy in the World of Internet of Things
#IoTPrivacy
#ATTPolicyForum

A panel of speakers discuss privacy in the age of IoT at the AT&T Policy Forum held at CMU.

Partnerships Lead to Safer Technology

Here at CyLab, we are redefining security in this increasingly connected world with forward-thinking, rigorous academic research. Through our corporate and institutional partners program, our researchers partner with government and industry to advance research and education in security and privacy. CyLab is supported by both public and private funding, predominantly government research funds, and the support of our corporate partners.

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 law enforcement agencies in other countries. Every partnership is united by a passion to create a world in which technology can be trusted.

To learn more about partnering with CyLab, please reach out to Michael Lisanti, Director of Partnerships, at mlisanti@andrew.cmu.edu or +1 412 268 1870

aetna®

AST
Allegheny Science & Technology

AT&T

aws

BOEING

EATON
Powering Business Worldwide

facebook

infineon

IR Ingersoll Rand
Inspiring Progress™

leidos

LG Electronics

Microsoft

MITSUBISHI
HEAVY INDUSTRIES

National Police Agency
JAPAN

NATO HQ
C3 Staff

NOKIA Bell Labs

NORTHROP GRUMMAN

Sandia
National
Laboratories

SIEMENS
Ingenuity for life

Symantec.™

T · · Mobile ·

UPMC LIFE CHANGING MEDICINE

CyLab News Briefs

AUG 30

State Department selects CyLab's Skinner as senior policy adviser

CyLab fellow Kiron Skinner, the Taube Professor of International Relations and Politics at Carnegie Mellon University, has been named senior policy adviser to U.S. Secretary of State Mike Pompeo.

SEP 07

CyLab study: Romantic couples are sharing online accounts in security-compromising ways

A CyLab research team surveyed 195 participants about their relationship status and account-sharing behavior across popular websites. The survey revealed users engaging in unsafe security practices.

SEP 17

CyLab launches initiative on IoT security

The IoT@CyLab initiative will bring together faculty and student researchers across the university and leading corporations with a common vision of making IoT more secure and privacy-respecting.

SEP 21

CyLab study finds users may be over-confident in protections of private browsing

A team of researchers from the CyLab Usable Privacy and Security Lab analyzed 450 consenting users' browsing behaviors over a three-year period. Their study was presented at last month's Symposium on Usable Privacy and Security in Baltimore.

SEP 27

Reducing complexity to increase security

CMU team received a $7.5M ONR grant for software complexity reduction, or simplifying complex internet protocols to build greater security.

SEP 28

CyLab launches massive middle and high school hacking competition, picoCTF

Guidance counselors today are urging their students to consider becoming doctors, lawyers, engineers, and ... computer hackers? That's the goal with picoCTF, Carnegie Mellon University's free, online cybersecurity competition for middle and high school students, which launches today for the fourth time since its inception in 2013.

OCT 15

CyLab researchers win NSA's Best Scientific Cybersecurity Paper competition

Two CyLab researchers led a study that has been named 2017's Best Scientific Cybersecurity Paper by NSA's Science of Security initiative.

OCT 19

Dena Haritos Tsamitis secures $5 million NSF award for CyberCorps Scholarship for Service

At a time when demand for cybersecurity expertise has never been higher, CMU has just been awarded a $5 million renewal of its National Science Foundation (NSF) CyberCorps Scholarship for Service (SFS) program through 2023.

OCT 24

CyLab faculty win big at the IEEE Cybersecurity Development Conference

CyLab faculty members Alessandro Acquisti, Lujo Bauer, Nicolas Christin, and Lorrie Cranor were presented with IEEE Cybersecurity awards at the IEEE Cybersecurity Development Conference, Oct. 2.

OCT 25

Advancing women in cybersecurity

At CMU, the Information Networking Institute is closing the cybersecurity gender gap one student at a time.

OCT 30

CyLab's Norman Sadeh speaks on plenary panel about data protection and privacy

Last week, CyLab's Norman Sadeh spoke about privacy, artificial intelligence (AI), and the challenges at the intersection of the two at the International Conference of Data Protection and Privacy Commissioners (ICDPPC).

DEC 05

Preventing exposure to malicious websites

A team of CyLab researchers have developed a mechanism that detects when users may be about to visit a malicious website.

DEC 11

Thwarting bias in AI systems

As machine learning systems are used increasingly to make decisions about insurance, criminal justice, credit, and child welfare, we need to ensure that they are fair.

DEC 17

Forging a user-friendly blockchain

In May of 2016 a thief was able to steal over $50 million in broad daylight from a pool of over 11,000 investors using a single line of poorly written code.

JAN 14

Lorrie Faith Cranor named new director of Carnegie Mellon University's CyLab

Lorrie Faith Cranor has been named the next director of CyLab, CMU's security and privacy institute, effective January 15.

JAN 30

Building a verifiably-secure internet

In security, almost nothing is guaranteed. It's impossible to test the infinite ways a criminal may penetrate a proverbial firewall. But what if, by the laws of mathematics, something could be proven to be secure without running an infinite number of tests?

FEB 19

CyLab study: How the Twitter community stopped fake news about "Black Panther"

On February 16, 2018, mere hours after Academy Award-nominated "Black Panther" first released to theaters, fake news trolls and malicious social media bots went to work.

MAR 05

CyLab's Gligor and Woo receive Distinguished Paper Award for breakthrough result on establishing "root of trust"

In a breakthrough study, "Establishing Root of Trust Unconditionally," CyLab researchers Virgil Gligor and Maverick Woo present a test that can be run on any computing device to show whether the device has been infected with malware or not.

MAR 08

Eight Carnegie Mellon faculty and staspoke at this week's RSA Conference

CMU had a big showing at this week's RSA Conference in San Francisco with eight faculty and staff members from across the university spoke about topics ranging from security and human behavior to the security of robot-produced code.

MAR 11

Blockchain Course Challenges Students To Create Apps for the Launch of CMU Cryptocurrency

CMU researchers are tapping into many disparate applications of blockchain and cryptography to advance economic and business functions of this new technology.

MAR 14

CMU partners with leading payments company Ripple to accelerate innovation in blockchain & cryptocurrency

CMU has announced a partnership with Ripple's University Blockchain Research Initiative (UBRI) to support academic research, technical development and innovation in blockchain, cryptocurrency and digital payments.

MAR 26

Celebrating women in cybersecurity

CMU's Lorrie Cranor and Dena Haritos Tsamitis will speak at this week's Women in Cybersecurity Conference in Pittsburgh.

APR 04

Achieving provably-secure encryption

Researchers from CyLab released the world's first verifiably secure industrial-strength cryptographic library – a set of code that can be used to protect data and is guaranteed to protect against the most popular classes of cyberattacks.

APR 18

A new era for the Bosch Chair

Lorrie Cranor has received the Bosch Distinguished Professorship in Security and Privacy Technologies, enabling her to lead a new era of security and privacy research at the university.

APR 23

Lorrie Cranor, Brian Kovak Named Andrew Carnegie Fellows

Carnegie Mellon University faculty members Lorrie Cranor and Brian K. Kovak have been named to the 2019 Class of Andrew Carnegie Fellows by the Carnegie Corporation of New York, a philanthropic foundation that has supported the advancement of education and knowledge for more than a century.

APR 29

First round of Secure and Private IoT Initiative funded projects announced

CyLab's Secure and Private IoT Initiative (IoT@CyLab) has broken ground as the first round of funded proposals have been announced. Twelve selected projects will be funded for one year.

MAY 07

Heinz College students conquer Deloitte Cyber Threat Competition

Four Heinz College of Information Systems and Public Policy students won top honors at the 2019 Deloitte Cyber Threat Competition by thwarting a simulated cyber attack.

MAY 10

Working with big data just got easier

Daehyeok Kim developed FreeFlow, an open-sourced software-based solution that unites two techniques that minimize disruption of cloud servers' central processing units (CPUs).

MAY 17

Blame the tech, not the users

A recent study led by researchers in CMU's CyLab found that when a personal device has fallen victim to some sort of cyberattack, users often misdiagnose what exactly is going on– but they're not the ones to blame.

MAY 30

BUYER UNAWARE: Security and privacy rarely considered before buying IoT devices

In a study presented at the ACM CHI conference, researchers from CyLab found that security and privacy risks may not be on the list of considerations when consumers purchase new IoT devices.

JUN 18

Securing the energy grid with blockchains

The US Department of Energy has awarded two Carnegie Mellon researchers a $400,000 grant to strengthen grid security using blockchain technology.

JUN 21

How to teach cybersecurity without scaring students away

Last week, the masterminds behind picoCTF shared some lessons learned in a paper at the Colloquium for Information System Security Education conference in Las Vegas.

JUN 28

Overcoming the privacy paradox

Why do some people say they value their privacy, but then willingly give up personal information when downloading an app? Understanding this so-called "privacy paradox" would help answer lots of questions about how privacy could be better dealt with.

JUL 08

Ads, cookies, and the EU privacy law

A team of researchers from CMU, the University of Minnesota, and the University of Paris-Sud have been pondering how the European Union's General Data Protection Regulation affected the use of cookies, as well as its impact on websites that rely on cookies for revenue-generating ads.

JUL 10

Malicious social media bots tried, but failed, to diminish NATO during its 2018 exercise

A new study by CMU researchers illustrates how fake news was spread on Twitter by bots during NATO's 2018 Trident Juncture Exercise. The study is being presented this week at the 2019 SBP-BRiMS conference in Washington, D.C.

JUL 11

Social media bots interfere in Asia-Pacific elections, too

Researchers from CMU wondered: are bots also influencing elections in the Asia-Pacific? Of course they are, says a new study being presented this week at the 2019 SBP-BRiMS conference in Washington, D.C.

JUL 18

NSF awards $1.2M to create a digital assistant to answer privacy questions

The National Science Foundation (NSF) awarded a $1.2 million grant to a team of researchers from CMU, Fordham University, and Penn State University to develop a tool – a "privacy assistant" – that will allow users to simply ask questions about the privacy issues that matter to them.

AUG 07

CMU's Plaid Parliament of Pwning prepares for DefCon 27

Five INI students and alums are headed to DefCon 2019 to compete in "World Series of Hacking."

AUG 12

CMU crowned hacking champs for fifth time in seven years

Carnegie Mellon University's competitive hacking team, the Plaid Parliament of Pwning (PPP), just won its fifth hacking world championship in seven years at this year's DefCon security conference.

AUG 15

Opting out of data use is hard, but it doesn't have to be

A recent study by researchers from CMU and the University of Michigan found that while many websites share users' browsing data with advertisers, it is difficult for users to figure out how to prevent this practice.

AUG 16

Why people (don't) use password managers effectively

A recent study by CyLab researchers provides some insight into how ineffectively people may be using password managers, potentially nullifying the benefits the managers are meant to provide.

AUG 19

Apps are rife with privacy compliance issues, and here's some evidence

A team of researchers from CMU and Fordham University recently created the Mobile App Privacy System (MAPS), a tool that uses natural language processing, machine learning, and code analysis to identify potential privacy compliance issues by inspecting apps' privacy policies and code.

AUG 22

When privacy and the arts collide

Sophie Calle is a French artist who often blurs the lines between life and her art. What if Calle knew how to code, and took advantage of our personal data to create an even more personalized, privacy-intrusive form of art? That's something CyLab's Maggie Oates has been exploring.

AUG 23

CyLab researchers create tool to help prevent cyberattacks on vehicles

CyLab's Sekar Kulandaivel and colleagues have developed a network-mapping tool to help keep vehicles protected from cyberattacks. The tool meticulously maps a car's network in under 30 minutes on less than $50 worth of hardware.

AUG 29

CyLab team uses AI to find and disrupt malware distribution networks

According to a new study authored by researchers in CyLab, network analysts have a new ally in detecting malware distribution networks: artificial intelligence.

15 Years of CyLab

This year, we celebrated 15 years since our founding. Here is a selection of milestones that CyLab's faculty, staff and students have achieved in our 15 years of working towards creating a world in which technology can be trusted.

Oct. 2003: CyLab was founded with a $6.1 million per year grant from the Army Research Office, creating one of the largest security and privacy research and education institutions of its time. CyLab was originally led by director Pradeep Khosla and director of education, training and outreach Dena Haritos Tsamitis. Mike Reiter served as the founding technical director.

2003-2004: Adrian Perrig, Dawn Song and others published a series of papers on secure protocols for sensor networks, which served as precursors to today's networks of IoT devices. Secure communication is a cornerstone of IoT device security.

May 2004: Lockheed Martin became CyLab's first corporate member, giving $25,000 to support ongoing research and development in cybersecurity and to educate the public on cybersecurity issues. CyLab's partners program would grow to over 20 corporate and government partners in 2019.

September 2004: CyLab launched a new executive security program at CMU's Silicon Valley campus to address the policy, management, and physical and technical issues facing government and industry.

September 2004: CMU team led by Mike Reiter was awarded a $6.4 million NSF grant to establish a new center, "Security Through Interaction Modeling" (STIM), housed in CyLab. In the same way that ecology studies the web of life, STIM aimed to understand and model the complex interactions among humans, computers, and attacks.

November 2004: Officials from the Korea Information Security Agency pledged $6 million over three years to form CyLab-Korea in Seoul, South Korea. A year later, CyLab would partner with the Hyogo Prefectural government to create the INI Kobe Master of Science in IT at CyLab-Japan.

2005: CyLab moved into the Collaboration Innovation Center on the CMU Pittsburgh campus, gaining 25,000 square feet of space to house faculty, staff, students, and meeting and lab space. The building was equipped with a smartphone-based distributed access control system, allowing faculty and staff to unlock their office doors with their smartphones before the term "smartphone" was commonly used. The system, named "Grey," was developed by Lujo Bauer and Mike Reiter.

April 2005: INI and CyLab launched MySecureCyberSpace.com, an initiative funded by the NSF to educate the public about computer security and internet safety. Dena Haritos Tsamitis served as the initiative's principal investigator.

2005: Seminal work on anti-phishing techniques began in CyLab. In 2008, Lorrie Cranor, Jason Hong, and Norman Sadeh turned their work into Wombat Security, a startup focusing on security awareness training to prevent phishing attacks. In 2018, the company was acquired by security company Proofpoint for $225 million.

2005: CyLab hosted the Symposium On Usable Privacy and Security (SOUPS), founded by Lorrie Cranor. SOUPS was the first conference focused on this topic. USENIX would eventually adopt SOUPS as one of their annual meetings.

2005: Nearly half of the papers at the annual IEEE Security and Privacy Symposium were co-authored by researchers from CyLab.

2008: Virgil Gligor became 2nd director of CyLab.

2008: Mike Reiter, Adrian Perrig, Bryan Parno, and Jonathan McCune proposed the Flicker system, which was a precursor to how we use trusted computing (e.g., SGX) today, allowing one to run a secure computation with added certainty that it's not being corrupted.

Wombat co-founders and early employees in 2009.

2009: Northrop Grumman established the Cybersecurity Research Consortium, working with CyLab, MIT, and Purdue University to enhance their cybersecurity abilities.

2009: Seeing-is-believing pairing protocol by Mike Reiter and Adrian Perrig showed how to use 2D barcodes to securely pair devices via a smartphone. Similar protocols are used today by many home IoT devices.

August 2009: A team of CyLab faculty were awarded a $3 million NSF grant to establish a usable privacy and security doctoral training program. This grant supported an interdisciplinary group of 27 students from four departments over eight years.

2010: Bryan Parno and colleagues introduced and formalized the term "verifiable computation," which enables a computer to offload computation to untrusted clients while maintaining verifiable results, paramount in cloud computing and client-server computing.

2011: David Brumley received the Presidential Early Career Award for Scientists and Engineers, the highest honor bestowed by the U.S. government on young scientists and engineers. He was honored for his "innovation and vital research on malware analysis and for strong educational and outreach activities."

2012: Nicolas Christin published the first extensive look into the economics of the Silk Road, an online anonymous marketplace that deals with drugs and other contraband. The FBI subsequently shut Silk Road down the following year.

2013: CyLab launched picoCTF, a free, online cybersecurity competition for middle and high school students. picoCTF would quickly become the largest competition of its kind with over 100,000 student participants to-date, many of whom were inspired to pursue cybersecurity in college.

2013: CMU launched the first of its kind Master's Program in Privacy Engineering to prepare students with technology backgrounds to develop products and services that respect user privacy.

2013: CyLab's competitive hacking team, the Plaid Parliament of Pwning (aka "PPP") won their first DefCon Capture the Flag competition. The competition is widely considered the "World Cup of Hacking," bringing together hacking teams from all over the world. PPP would eventually win four more DefCon titles (2014, 2016, 2017, and 2019), making them the winningest team in DefCon history.

2013: Jason Hong developed PrivacyGrade.org, a website that assigns letter grades to apps based on how they treat users' data. Subsequently, the FTC charges that the developer of the Android Flashlight App, one of the most popular Android apps at the time, deceived consumers about its data practices.

2014: A CyLab team won DefCon's "Crack me if you can" password-cracking challenge, combining multiple cracking approaches to crack more passwords than any of their competitors. The same researchers would eventually go on to develop and win Best Paper Awards for a machine-learning-based tool to calculate password strength (USENIX Security, 2016) and a password creation interface that helps users create stronger, but still memorable, passwords (ACM CHI, 2017).

October 2015: Two CyLab teams were awarded DARPA Brandeis grants. Norman Sadeh and colleagues' project focuses on personalized privacy assistants that can assist smartphone users in protecting their privacy. Jason Hong and colleagues are working on improving the privacy of Android smartphones with new ways of analyzing app behaviors, developer support, and user interfaces.

2015: David Brumley became 3rd director of CyLab. He also became CyLab's first Bosch Distinguished Professor in Security and Privacy Technologies, a position to be held by the CyLab director.

2016: David Brumley's startup, ForAllSecure, advanced CyLab research on automated attacks to win the 2016 DARPA Cyber Grand Challenge, a first-of-its-kind completely autonomous hacking competition. The team received $2 million in prize money.

2016: Lujo Bauer and colleagues demonstrated the first physically realizable attacks on a machine learning-based system, using custom eyeglass frames to fool state-of-the-art facial-recognition systems.

2016-2017: Virgil Gligor led work to establish what is known as a "root of trust," creating a test that — for the first time ever — could detect malware on a device with near certainty. The study received a Distinguished Paper Award (NDSS, 2019), and Gligor would be inducted into the Cybersecurity Hall of Fame for this work and others in 2019.

2017: Doug Sicker became the interim director of CyLab while David Brumley went on-leave to grow his startup, ForAllSecure.

2018: CyLab launched the Secure and Private IoT initiative, co-directed by Vyas Sekar and Anthony Rowe, with founding sponsors Amazon Web Services, AT&T, Infineon Technologies, and Nokia Bell Labs. At a time when the number of IoT devices is exploding, CyLab's IoT initiative aimed to create the knowledge and capabilities to build secure and privacy-respecting IoT systems.

2018: A team led by Lujo Bauer, Nicolas Christin, Lorrie Cranor was awarded the IEEE Cybersecurity Award for Practice in recognition of their massive body of research on password security. Alessandro Acquisti was awarded the IEEE Cybersecurity Award for Innovation for his groundbreaking work on the economics and behavioral economics of privacy and personal information security.

2018: Norman Sadeh and colleagues successfully executed the first-ever automated analysis of over 1 million mobile apps for privacy compliance to analyze the text of privacy policies and code analysis techniques.

2018: The $27.5 million CONIX Center was established at CMU to build smarter networks to connect edge devices to the cloud, with CyLab's Anthony Rowe as director.

2018: Marios Savvides' startup HawXeye was acquired by Bossa Nova Robotics to make their aisle-roaming robots smarter. Their robots were in over 50 Walmart stores around the country at the time, scanning shelves for out-of-stock or misplaced products.

2018: CMU launched a security and privacy concentration to undergraduates in computer science and in electrical and computer engineering.

2018: David Brumley and recent graduate Tiffany Bao won the NSA's 6th Annual Best Scientific Cybersecurity Paper Competition for their paper on the impact of information sources on code security. Previously, CyLab researchers won the 4th Annual competition and received honorable mention in the 3rd annual competition.

2019: Lorrie Cranor became the 4th director of CyLab.

2019: Kathleen Carley, Doug Sicker, and David Danks were awarded a $5M grant from the Knight Foundation to launch the Center for Informed Democracy and Social Cybersecurity to foster research around topics such as how to better recognize disinformation online, how to identify who is spreading it, how to inoculate groups against it, and how to counter it.

David Brumley (third from left) celebrates on stage with his startup, ForAllSecure, for winning the DARPA Cyber Grand Challenge in 2016. The team used CyLab-born technologies to create an autonomous hacking system that out-hacked six other qualifying teams.

Carnegie Mellon Security + Privacy

CyLab