YEAR IN REVIEW

Carnegie Mellon University
Software Engineering Institute

The Software Engineering Institute (SEI) is a federally funded research and development center (FFRDC) sponsored by the U.S. Department of Defense and operated by Carnegie Mellon University.

The SEI's mission is to advance the technologies and practices needed to acquire, develop, operate, and sustain software systems that are innovative, affordable, trustworthy, and enduring.

The 2018 *SEI Year in Review* highlights the work of the institute undertaken during the fiscal year spanning October 1, 2017, to September 30, 2018.

A Message from the Director and Chief Executive Officer

Maintaining a technological advantage over our adversaries is crucial to our nation's security, but software complexity, scale, and security; legacy development processes; and the regulatory and oversight environment in which new capabilities arise (to name just a few) all pose significant challenges to the mission of the Department of Defense (DoD). Hurdles such as these impede the DoD's ability to field new capabilities—so many of which are software-reliant—at the pace necessary to maintain our competitive edge.

Machine learning (ML) and artificial intelligence (AI); a revamped software factory model informed by contemporary tool chains; and iterative development practices, such as Agile and DevOps, all have created opportunities to surmount these challenges and, as you will read in this year's edition of the *Year in Review*, the SEI has been hard at work on numerous research and development efforts in these areas.

Our ML and AI portfolio has been growing quickly over the past several years, particularly in the area of narrow AI, and we are also driving advances in the field of engineering for AI, including in such areas as AI safety and security, acquisition transformation, and AI for software engineering. We've also made concrete advances on video search and summarization techniques, real-time extraction of biometric data from video, automated software evolution, and computer vision.

Because of our research leadership concerning the adoption of Agile and DevOps in DoD environments, the Office of the Secretary of Defense called on the SEI to contribute to several key initiatives in the 2018 National Defense Authorization Act. One of these initiatives addresses streamlining acquisition practices, and two involve pilot programs aimed at understanding Agile adoption and the use of Agile in long-term defense projects. Alongside our Agile efforts, our work in the area of secure DevOps demonstrates how cybersecurity, long viewed as a roadblock to rapid deployment of new software-based capabilities, can be addressed in a DevOps platform while maintaining quality, reliability, and pace of deployment.

These are just a few examples of the important work undertaken by the men and women of the SEI in fiscal year 2018. I'm pleased to present the 2018 *Year in Review*, and I encourage you to read more about how we're advancing the field of software engineering in the age of AI.

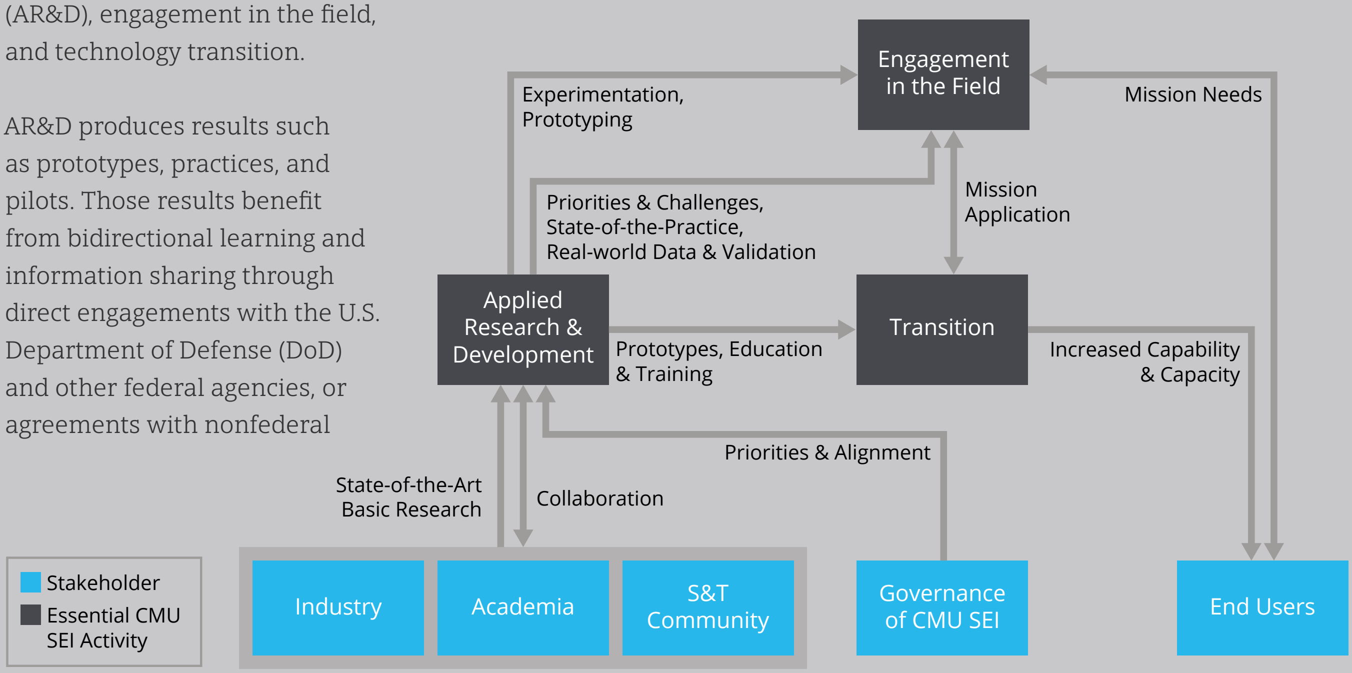
Paul D. Nielsen
Director and CEO

Execution Strategy

The SEI employs an agile execution strategy, directing resources to the most critical ongoing and future challenges. This approach applies advances in technology and new insights to meet immediate needs, while developing capabilities to address larger underlying material and nonmaterial problems. The organization's essential activities are applied research and development (AR&D), engagement in the field, and technology transition.

AR&D produces results such as prototypes, practices, and pilots. Those results benefit from bidirectional learning and information sharing through direct engagements with the U.S. Department of Defense (DoD) and other federal agencies, or agreements with nonfederal and commercial organizations. The SEI engages with customer organizations that have high-priority challenges and problems it can address by closing lifecycle technology gaps. Direct engagement enhances AR&D activities with an understanding of the state of the practice, current and future challenges and gaps, adoption considerations, and access to real-world data and environments that support experimentation, validation, and the maturation of research approaches.

These engagements also provide the credibility and access that enable technology transfer to DoD organizations and the wider software engineering community.


Engagement in the Field
Experimentation, Prototyping
Mission Needs
Priorities & Challenges, State-of-the-Practice, Real-world Data & Validation
Mission Application
Applied Research & Development
Prototypes, Education & Training
Transition
Increased Capability & Capacity
Priorities & Alignment
State-of-the-Art Basic Research
Collaboration
🟦 Stakeholder
⬛ Essential CMU SEI Activity
Industry
Academia
S&T Community
Governance of CMU SEI
End Users

FUNDING SOURCES

In FY 2018, the SEI received funding from a variety of sources in the Department of Defense, civil agencies, and industry.

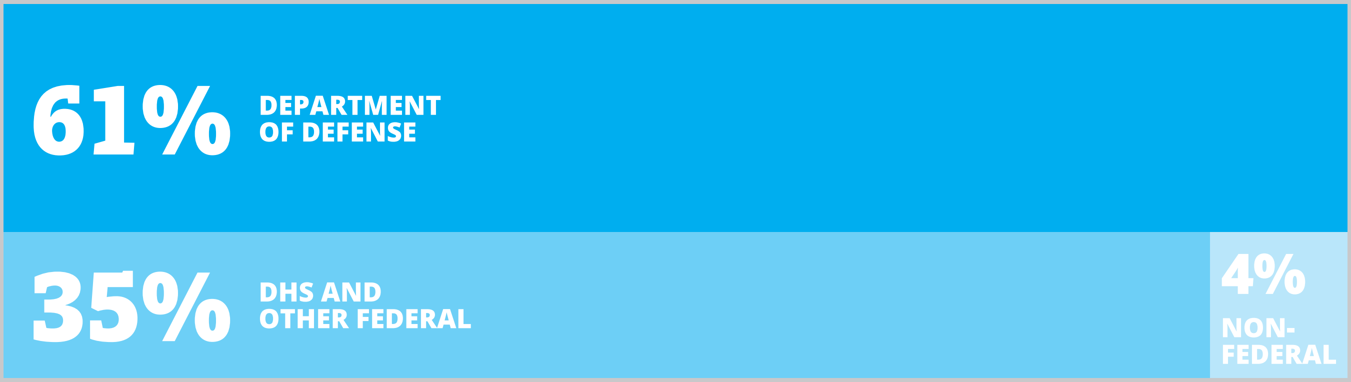


Table of Contents

SEI News

LONGSTAFF RETURNS TO SEI AS CHIEF TECHNOLOGY OFFICER

The SEI welcomed back a familiar face in 2018 with the appointment of nationally known cybersecurity researcher Tom Longstaff as chief technology officer (CTO). In his new role, Longstaff will formulate the SEI's technical strategy and lead the institute's funded research program.

Longstaff most recently served as program manager and principal cybersecurity strategist for the Asymmetric Operations Sector of the Johns Hopkins University Applied Physics Laboratory (APL), where he led projects on behalf of the U.S. government. Prior to joining APL, Longstaff was the SEI CERT Division's deputy director for technology. In his 15 years at the SEI, he helped shape the program into an internationally recognized network security organization.

"The role of the chief technology officer is critical in ensuring we have the proper technology strategy in place to help the Department of Defense and our other sponsors, both now and into the future," said Dr. Paul Nielsen, SEI director and CEO. "Because of Tom's previous service at the SEI, he is uniquely suited to direct our current research and plan its future direction."

For more on Tom Longstaff and his vision for future SEI research, see the article "Longstaff Returns to Take the Reins as CTO."

MAGNELIA NAMED CFO

In September 2018, the SEI introduced Heidi S. Magnelia as its new chief financial officer (CFO). Magnelia brings more than 30 years of experience as a financial professional to the SEI and has previous experience in government-funded research, consulting, and commercial organizations.

"We're glad to welcome Heidi to the SEI," said Paul Nielsen, SEI director and CEO. "Her experience as a financial manager at government-funded research organizations means she has a deep understanding of our mission to provide technology solutions to support national defense."

Prior to joining the SEI, she served in a number of fiscal roles at MITRE Corp. in McLean, Virginia.

"As a Pittsburgh native, I'm glad to be able to return home and to make my contribution to both Carnegie Mellon University, a global leader in technology research and education, and the Software Engineering Institute, which makes critical contributions to national security through its research in software engineering and cybersecurity," said Magnelia.

SEI STAFF ASSUME KEY EDITORSHIPS

The SEI's Ipek Ozkaya and Leigh Metcalf assumed editorships in 2018. Ozkaya, a principal researcher in the SEI's Software Solutions Division, was named editor-in-chief of *IEEE Software*, a leading bimonthly peer-reviewed journal published by the IEEE Computer Society. Metcalf, a senior network security research analyst specializing in cybersecurity, is founder and co-editor-in-chief of *Digital Threats: Research and Practice (DTRAP),* a journal of the Association for Computing Machinery.

Ozkaya assumed editorial duties in January 2019. She plans to focus on publishing results that provide practical guidance and help for both established and newcomer software developers and architects. For all practitioners, Ozkaya plans to work toward the transition of practical research through easily consumable means.

By establishing *DTRAP*, Metcalf seeks to promote the foundational development of scientific rigor in digital security by bridging the gap between academic research and industry practice. *DTRAP* launched in January 2019.

For more information about IEEE Software, visit **publications.computer.org/software-magazine**

For more information about *DTRAP*, visit **dtrap.acm.org**.

SHULL ELECTED IEEE COMPUTER SOCIETY FIRST VICE PRESIDENT

Forrest Shull, assistant director for empirical research in the Software Solutions Division of the SEI, was elected first vice president of the IEEE Computer Society. Shull will work directly with the IEEE Computer Society president and other leaders who manage the society's technical offerings, which include conferences, publications, technical communities, education, and standards. He will also provide advice and leadership at a strategic level.

"Throughout my time volunteering with the Computer Society, I've been able to see firsthand the many activities we support, literally around the world, that grow and support the technical community," said Shull, who served the IEEE Computer Society for several years in several different roles.

As first vice president, Shull plans to continue to work on ways to improve the society's connections to its members and adapt its offerings to meet the evolving expectations of the society's membership. "My work here at the SEI helps keep me connected to customers and stakeholders who are working on innovative systems. They're hungry for the practical knowledge that can help them get where they need to go, which is a good reminder of the overall mission of the society itself."

Longstaff Returns to Take the Reins as CTO

In 2018, the SEI announced the appointment of nationally known cybersecurity researcher Tom Longstaff as its chief technology officer (CTO). The appointment marked a homecoming of sorts for Longstaff who, in an earlier tenure that spanned 15 years, helped the SEI's CERT Division become an internationally recognized cybersecurity organization.

Prior to his return to the SEI, Longstaff was a program manager and principal cybersecurity strategist for the Asymmetric Operations Sector of the Johns Hopkins University Applied Physics Laboratory (APL). He also is former chair of the Computer Science, Cybersecurity, and Information Systems Engineering programs and co-chair of Data Science in the Whiting School at Johns Hopkins. Longstaff joined the staff at APL after having served the SEI as the deputy director for technology for the CERT Division.

"The role of the chief technology officer is critical in ensuring that we have the proper technology strategy in place to help the Department of Defense and our other sponsors ensure critical systems both now and into the future," said Dr. Paul Nielsen, SEI director and CEO. "Because of Tom's previous service in the SEI's CERT Division, he is uniquely suited to direct our current research and plan future direction."

As CTO, Longstaff will formulate a technical strategy and lead the SEI's funded research program based on current and predicted future trends in technology, government, and industry. Longstaff sees a direct progression from where the SEI has been, where it is, and where it is going.

"At its inception, beginning with the software development process work we became known for, the work of the SEI was based on measuring things that no one had ever measured before," said Longstaff. "Real data and real measurement informed our software processes and the other advances we were working on."

Measurement and data were also critical to the next step in the SEI's evolution: the creation of the CERT Division and the move into cybersecurity. "We created tools to measure network activity and find out exactly what was going on," said Longstaff. "We captured data and used it to drive our research and development, not only for cybersecurity but also for things like software architecture and product line development."

Longstaff sees the SEI now moving into a new phase of its evolution. "We're in a new world where software is the ocean that everything swims in," he said. "It's a world based on software and data, and it's driven by artificial intelligence [AI], especially machine learning, and data science.

"I believe the SEI is well positioned to play a leading role in this space, not just in terms of how it can be used to create new capabilities but also in how AI can be used to revolutionize the way we compose software itself—to do it faster, better, more efficiently, and with fewer vulnerabilities, problems, and faults.

"We need to help our sponsors in the Department of Defense understand this new world, to help them make the shift from a world in which everything revolved around hardware to one in which

everything revolves around a hardware-software partnership, a world in which collecting and understanding sensor data plays a significant role in the operational deployment of new capabilities."

In the near term, Longstaff sees the SEI aligning to the challenges of this future world. One advantage here is the institute's close alignment with Carnegie Mellon University (CMU). "I see the SEI as the linchpin between the DoD's mission and the academic research going on at CMU. By anybody's estimate, Carnegie Mellon is the leader in AI and data-related research. We develop capability, we invent new technologies, but we also work with the university in those areas where they have unique academic expertise."

Longstaff's approach to his new role is animated by passion for what he does and a sense of excitement about the ways in which the SEI can help the DoD, and by extension our nation and the world, meet the challenges of a rapidly evolving technological landscape.

Today’s CERT Division Works to Simplify Cybersecurity

CERT Division Director Bobbie Stempfley describes the SEI’s priorities in finding and transitioning solutions for today’s cybersecurity challenges.

When you look at the challenge of cybersecurity, it’s easy to feel overwhelmed by the scale and complexity of the problems we face, and the speed at which everything changes.

Our instinct is to “complexify” everything. So instead, at the SEI CERT Division, we try to simplify.

Our adversaries are going after a small set of things:

Software design tradeoffs. When we architect and build systems, there is never enough time, money, power, or resources, so we make design tradeoffs. Our adversaries look for the opportunities those tradeoffs create.

Failures in implementation. Something didn’t quite get built the way we thought it would, and we—and our adversaries—understand those failures as vulnerabilities.

Tunnel vision in use cases. We build a technology to do a particular thing. We might test it for edge cases. But the end user, who might be an18-year-old sailor, will inevitably use it in ways we never imagined. Our adversaries look for those cases of unintended use.

The seams between efforts and activities. We know these things as race conditions or side-channel-related activities. Two pieces of software exchange data; that’s a seam. Or, one chip runs at a particular speed, and another chip runs at a different speed. That creates an environment that you didn’t expect. In today’s complex systems, there are a lot of these seams.

If you look at it this way, it helps you focus on the things you need to fix. We recognize that we cannot engineer or buy our way out of these problems. So we take a holistic approach to solving today’s challenges, which requires us to think more deeply and strategically about where and how to engage.

Instead of chasing every vulnerability, we chase answers to questions such as how do I build things better? How do we work with Agile concepts to bring security into development activities? How do we build secure concepts for coding? How do we reduce the implementation risks in that space? How do we help operators understand their roles in the environment? How do we understand enterprise risk so we have continuity of practice, completeness of practice, and efficacy of practice? And then, how do we really focus on simplification as often as possible?

At the SEI CERT Division, we do research to find answers that will scale. We promote those answers through training, documented standards, and other mechanisms for the broader community. We also focus on development of the cyber workforce, those defenders and administrators in the national security space who need to understand how to do their jobs.

We still analyze malware and vulnerabilities, but with the goal of speeding up the distribution of holistic solutions so that others can put protections in place.

U.S. Navy Unit Establishes Presence at SEI Headquarters

Cyberspace has become a theater of operations crucial to all branches of the armed forces. It's an environment that changes rapidly and in which new threats and challenges continually emerge and evolve. What's more, it touches nearly every facet of Department of Defense (DoD) operations, from acquisition to command and control to advanced weaponry.

Recognizing the need to keep pace with this dynamic cyberspace environment, the U.S. Fleet Cyber Command has stood up a detachment at the SEI's headquarters in Pittsburgh. According to Vice Admiral Michael M. Gilday, the objective of this reserve unit, which is attached to the Navy's Cyber Warfare Development Group, "is to better leverage the research and technology rising out of Carnegie Mellon University and the Software Engineering Institute." Gilday added, "This was initiated to better connect with advances in the academic world to enhance our cyber mission force training and cyber tool development."

In March 2018, testifying before the Senate Armed Services Committee, Subcommittee on Cybersecurity, Gilday discussed the challenges the current environment presents. Gilday heads up the U.S. Fleet Cyber Command, U.S. Tenth Fleet. He noted that "… our adversaries often act within the 'gray zone,' heavily relying on asymmetric methods such as cyberspace and information operations to undermine our national interests." Gilday added that operating at sea provides no refuge. "I have observed first-hand how the United States is threatened by cyber-attacks every day; the threat to the U.S. Navy is certainly no different," he said.

"We're excited to partner with the Navy on this mission, which is the first of its kind," said SEI Director and CEO Paul Nielsen. "While the primary purpose is to transfer skills and know-how to the U.S. Fleet Cyber Command, an engagement like this also provides our people a great opportunity to learn more about the challenges confronting the men and women working at the tactical edge."

To learn more about this and other topics discussed in the *Year in Review,* visit **resources.sei.cmu.edu** and search for "2018 SEI Year in Review Resources."

Photo: U.S. Navy

Section 872 Team Researchers (from top)
RHONDA BROWN, NICK GUERTIN, ANDY MOORE, BILL NOVAK, FORREST SHULL, AND DAVE ZUBROW

SEI Lends Agile Expertise in Support of Key NDAA Initiatives

With a focus on speeding the delivery of software capability to end users, the SEI has conducted research on Agile software approaches in the DoD and government settings since 2009. Our personnel well understand the challenges of Agile implementation in this specialized environment, and have assisted government stakeholders with adoption. This is why the SEI was tapped to lend its expertise in support of key initiatives mandated by Congress in the 2018 National Defense Authorization Act (NDAA), which contained provisions reflecting the growing recognition of the importance of software acquisition for the DoD's mission.

Section 872 of the NDAA established a study by the Defense Innovation Board focused on streamlining software development and acquisition regulations, which the SEI supports in multiple ways. Our team has developed case studies across the DoD to help identify legislative and policy changes needed to improve software acquisition in the ways needed to maintain the DoD's technological advantages over adversaries. This work focuses on topics that impact multiple stakeholders in the DoD acquisition ecosystem, such as the transition to continuous integration and continuous deployment, new workforce competencies, the "shifting left" of security accreditation and testing, and others.

The SEI also executed an analysis of DoD data collections related to software acquisition. Modern software analytics approaches are providing important results in industry, and our analysis explored how these technologies can be applied to better manage the quality, cost, and schedule required to deliver new software capabilities for defense.

Sections 873 and 874 call for pilot programs on the use of Agile methods. The pilots established are a mix of twelve-month efforts aimed at understanding issues with Agile adoption, as well as pilots on larger-scale programs that apply lessons learned over longer timeframes. The SEI serves on the core team responsible for the Office of the Secretary of Defense's execution of these pilot programs.

A necessary early step is to develop an understanding of program characteristics and contexts. Prior work with the DoD and other government agencies led the SEI to develop the Readiness and Fit Analysis, a model and method for understanding risks and enablers when contemplating or embarking on the adoption of new practices, such as Agile practices. The Readiness and Fit Analysis formed the basis of the core team's approach to characterize the pilot organizations and highlight potential challenges they need to overcome on the path to Agile adoption.

In both of these areas of work, the SEI team is providing leadership and subject matter expertise, interfacing with programs and other stakeholders across the

Sections 873–874 Researchers (from top)
WILL HAYES, SUZANNE MILLER, CRISANNE NOLAN, RICH TURNER, AND EILEEN WRUBEL

DoD acquisition ecosystem to streamline and improve the process for specifying, costing, testing, and accrediting software systems.

"In the current competitive environment, DoD programs are more than ever looking to exploit how software can enable frequent updates to system capabilities and allow us to maintain strategic overmatch against our adversaries," said Forrest Shull, assistant director of empirical research for the SEI's Software Solutions Division. "Agile is one of the keys to speeding the deployment of new DoD capabilities that can preserve its technological edge—achieving performance at the speed of relevance. These are high-visibility efforts, and we're pleased to have assembled two expert teams able to play such an important role in helping the DoD achieve these goals."

Photos (clockwise from top): U.S. Navy, U.S. Army, U.S. Marines Lance Cpl. Harrison Rakhshani , U.S. Air Force

Researchers
ROBERT CUNNINGHAM, BOBBIE STEMPFLEY, AND MATT GASTON

SEI Artificial Intelligence Portfolio Supports U.S. Information Dominance

To maintain its information dominance in the age of big data, the Department of Defense (DoD) will need to leverage artificial intelligence (AI) across its mission space. Recognizing this reality, the Defense Science Board (DSB), in its February 2018 report "Design and Acquisition of Software for Defense Systems," recommended that "DARPA, the SEI and DoD labs should establish research and experimentation programs around the practical use of machine learning in defense systems... ."

Even prior to the DSB's recommendations, however, the SEI had been building a portfolio of research and development in the areas of machine learning (ML) and AI. "The institute's focus has been on the realm of narrow AI, or single tasks a machine can perform better than a human," said Matt Gaston, director of the SEI's Emerging Technology Center (ETC) and a member of the SEI's AI Strategy team.

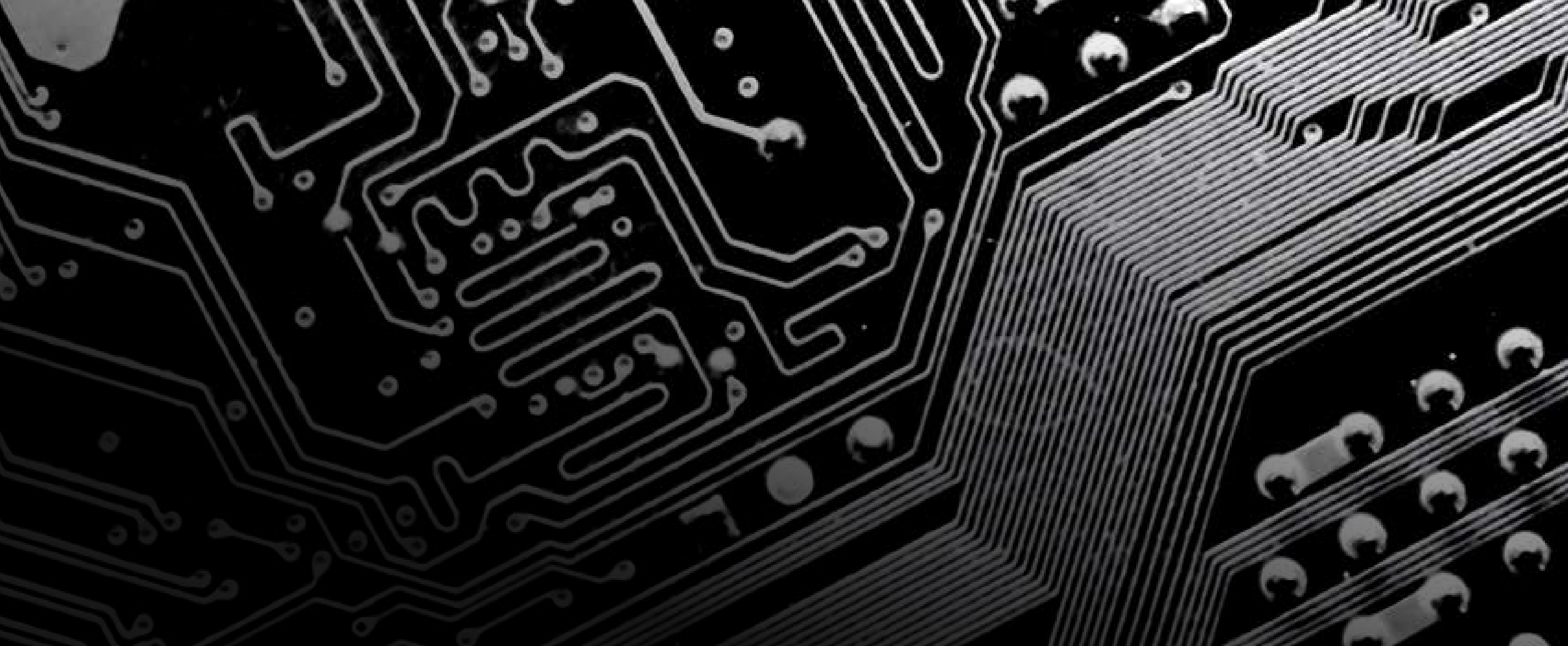
Narrow AI is particularly useful for making sense of large volumes of data, like reading and analyzing satellite imagery or generating models of future outcomes from years of historical data. "Accomplishing these narrow AI tasks and bringing AI capabilities to bear on mission challenges requires moving toward a mature discipline for AI engineering—an area where the SEI is uniquely positioned to contribute, given our expertise in maturing the discipline of software engineering," said Gaston.

> *"...bringing AI capabilities to bear on mission challenges requires moving toward a mature discipline for AI engineering..."*
>
> **—MATT GASTON, DIRECTOR, SEI EMERGING TECHNOLOGY CENTER**

Bobbie Stempfley, director of the SEI's CERT Division and chair of the AI Strategy team, sees several key challenges for AI development in DoD environments. "It's imperative to build and implement machine-learning algorithms with as few flaws as possible," she noted. "We have to recognize that they will be existing in contested space. This means the algorithm, the models, the data, and the mission context are all subject to adversary actions, both by humans and adversarial AI. Finally, we really need to understand and assure what happens to them over time, because they are going to evolve."

As part of Carnegie Mellon University (CMU), the SEI is particularly well positioned for this line of research. CMU is a recognized center for AI expertise, and *U.S. News & World Report* recently awarded CMU's artificial intelligence program its top ranking. This leadership was again recognized in 2018 when the U.S. Army's AI Task Force selected CMU as its hub for connecting the Army with the broader AI community.

SEI researchers, often in collaboration with their CMU



colleagues, have pursued a number of ML and AI projects applicable to DoD mission capabilities, such as intelligence, surveillance, and reconnaissance (ISR) and logistics. Examples of this work include the following:

Video search and summarization: Research by the SEI's Tactical Technologies Group examined how ML could be used to reduce unmanned aircraft system (UAS) workforce needs by automating tasks currently performed by humans. Specifically, the team examined using ML to automate the processing of UAS surveillance video.

Real-time extraction of heart rate from video: SEI researchers from the ETC designed and implemented algorithms to extract heart rate from video of non-stationary subjects' faces in practical settings in real time. Their work makes it possible to obtain heart rate information using only a standard web camera, and it employs facial landmarking to determine the region of interest where heart rate is most obvious. The SEI has also conducted related work on micro-expression recognition and detecting emotion from voice.

Cost-efficient maintenance: Maintenance of military hardware involves many thousands of units, often with a high cost per unit for items such as jet engine pulls. The need to reduce unscheduled and premature maintenance is great. To address this challenge, the SEI is using ML to create models capable of predicting degraded engine health to better determine and control the nature and timing of scheduled maintenance.

Automated software evolution (refactoring): Refactoring is slow and labor intensive. We are creating an automated component refactoring assistant to recommend architectural refactoring and implement it through code transformations.

Computer vision: A team of SEI, CMU, and University of Pittsburgh researchers applied innovative computer vision techniques to more quickly and accurately read satellite data imagery. Their adaptive "chipping" technique earned them a top-five spot in the Pentagon's Defense Innovation Unit Experimental Challenge in 2018.

Other notable work: The SEI has also been conducting research in the areas of certifiable distributed runtime assurance to ensure the safe behavior of autonomous systems, the use of deep learning to predict security vulnerabilities in synthetic code, the application of large-scale machine learning on big data, and the Robot Operating System-Military (ROS-M).

More broadly, the SEI has been advancing the field of engineering for AI. This includes work in the areas of

- data collocation and curation
- verification and validation of AI
- acquisition transformation
- monitoring for data drift and adversary actions
- AI for software engineering
- safety and security of AI

All of these efforts demonstrate the lead the SEI is taking in ML and AI research and the institute's commitment to making software a strategic advantage for the DoD.

To learn more about this and other topics discussed in the *Year in Review,* visit **resources.sei.cmu.edu** and search for "2018 SEI Year in Review Resources."

AFNOC Mission
Execute AFNETOPS/CC authority to command and control the operation and defense of the AF Network
AFNetOps C2 Relationship

Researchers
SAMUEL PERL, MATT SISK

CERT Tool Speeds Information Extraction and Analysis

Harried cybersecurity teams need to collect and process data from incident reports, blog posts, news feeds, threat reports, and many other sources. Names of technical artifacts, or technical observables, contained in these sources help analysts investigate threats and develop mitigations. But all too often this work involves manually cutting and pasting between sources and tools, a task that robs valuable time from limited analytical resources.

To relieve the analyst of this burden, the SEI's CERT Division has released Cyobstract, an open-source incident response tool. Cyobstract helps analysts quickly and efficiently extract information from any textual source or collection of sources, such as incident reports and the other sources noted above. The tool is freely available on GitHub.

"We created Cyobstract to support exploratory work we conducted on a dataset of Department of Homeland Security (DHS) incident reports," said Samuel Perl of the CERT CSIRT Development team and a developer of Cyobstract. "It streamlined the process by eliminating the need for a lot of cutting and pasting between data sources and tools. We quickly realized the tool could be of great help across the incident response analyst community."

Cyobstract targets 24 security-relevant data types, including IP addresses, hashes, Internet and system-related strings, Internet infrastructure values, and security analysis values. The tool can extract malformed or "defanged" values, and it also includes a developer kit teams can use to adapt the tool to capture custom security data types. But that's not all.

"Not only does it extract artifact-related information," said Matt Sisk, a colleague of Perl and co-developer of Cyobstract, "it also includes a tool that can automatically build optimized regular expressions from lists of target data."

> The Cyobstract library can be downloaded from GitHub at **github.com/cmu-sei/cyobstract**.

Photo: U.S. Air Force

Researchers
ANITA CARLETON, JOHN ROBERT, AND ERIN HARPER

Software as a Strategic Advantage

What will software engineering look like in the future? New concepts in automation will become reality, enabled by advances in analyzable architectures, software assurance, and artificial intelligence (AI). Automation will eliminate many tedious programming tasks. Code will be generated from verified models. Operational data will be used for runtime verification and to continually refine models. Innovations developed in the lab will be easily integrated and safely tested in the field. Ultimately, sources of troublesome behavior will be discovered and eliminated without human intervention, thanks to well-specified architecture semantics. In short, computers will become more than tools that execute exact specifications and will instead function more as colleagues.

Envisioning this new future is a key part of the SEI's work. "The ubiquity of software and its critical role require fundamental shifts in software engineering to maintain the DoD's competitive advantage," said Anita Carleton, acting director of the Software Solutions Division. "That motivates the SEI's software strategy."

According to a Defense Science Board report, software is among the most frequent and critical challenges for acquisition programs and drives risk on approximately 60 percent of programs. Since mission capability often requires software, software has become a national defense priority, supporting the mission outlined in the National Defense Strategy. "The central point of the SEI's software strategy is to ensure the DoD can rapidly deploy software innovations with confidence," said John Robert, deputy director of SSD. The SEI's strategy has three dimensions: engineering intelligent software systems, enabling DoD mission capability with software innovation, and informing DoD software policy and practice to accelerate acquisition.

Engineering intelligent systems requires the development of innovative architectures, analyses, algorithms, and tools. These solutions must work across many challenging system types used by the DoD, including tactical, cyber-physical, and AI systems. Integration will also require extending DevSecOps to build in assurance for rapidly deployable, mission critical systems.

Enabling DoD mission capability with software innovation means connecting research to practice and putting new solutions to work in DoD programs. Some of the SEI's work with DoD programs involves advanced video analysis using machine learning, enabling cloud computing at the tactical edge with cloudlets, and applying new approaches for automated testing and evaluation.

Informing DoD software policy and practice to accelerate acquisition is a key part of the SEI's mission. "Getting new technology into the field faster is how the DoD maintains its competitive advantage," said Carleton. No matter how innovative and promising, new software technologies and processes cannot affect the warfighter unless DoD acquisition policies—and ultimately the entire acquisition ecosystem—support their adoption.

Planning for the future is a challenge in the face of today's rapid technological change. "We have to closely monitor technologies, trends, and DoD priorities that have software engineering implications to keep our strategy fresh and positioned for the future," said Carleton. "Whether we're considering DevSecOps tool pipelines, new formal verification methods, or principles for the engineering of AI systems, we need to plan for innovation."

Researchers (from top)
MICHAEL KONRAD, ROBERT STODDARD, BILL NICHOLS, SARAH SHEARD, AND DAVE ZUBROW

From Correlation to Causation: Investigating the Sources of Software Cost

The Department of Defense (DoD) and its contractors often struggle with cost overruns in software development programs. To contain these costs, acquirers and developers must understand the factors that increase cost and can be controlled. Previous work has explored the correlation of many variables with cost. SEI principal researchers Michael Konrad and Robert Stoddard aim to move beyond correlation to causation in the Software Cost Prediction and Control (SCOPE) project.

SCOPE applies the open-source Tetrad tool's causal search algorithms to a large volume of project data to identify, measure, and test causality of cost. Among other sources, SCOPE analyzed data from DoD software projects reporting initial estimates and final actuals in the Systematic Review Data Repository. "The output is a graph," Konrad explained, "identifying which variables to manipulate to change particular outcomes of interest."

Working with Konrad and Stoddard were the SEI's Bill Nichols, Sarah Sheard, and Dave Zubrow as well as collaborators from the Carnegie Mellon University Departments of Philosophy and Psychology and the University of Southern California Center for Systems and Software Engineering.

Stoddard emphasized, "An immediate benefit is learning which factors have or do not have evidence supporting a causal path to software cost." Longer-term benefits include using the causal models to inform should-cost analysis, improve contract incentives, and control costs, schedule, and quality from development to sustainment.

> *"An immediate benefit is learning which factors have or do not have evidence supporting a causal path to software cost."*
>
> **—ROBERT STODDARD, PRINCIPAL RESEARCHER**

> To learn more about this and other topics discussed in the *Year in Review,* visit **resources.sei.cmu.edu** and search for "2018 SEI Year in Review Resources."

Photo: U.S. Air Force (above)

```
 rror_mod.      MIRROR_X":
mirror_mod.use_x = True
mirror_mod.use_y = False
mirror_mod.use_z = False
 _operation == "MIRROR_Y":
mirror_mod.use_x = False
mirror_mod.use_y = True
mirror_mod.use_z = False
 _operation == "MIRROR_Z":
mirror_mod.use_x = False
mirror_mod.use_y = False
mirror_mod.use_z = True

 election at the end -add
   _ob.select= 1
  ier_ob.select=1
  ntext.scene.objects.activ
  ("Selected" + str(modifier
  irror_ob.select = 0
 = bpy.context.selected_ob
 ata.objects[one.name].se

print("please select exactl

 -- OPERATOR CLASSES ----

types.Operator):
 X mirror to the selected
 ject.mirror_mirror_x"
 rror X"

 t):       ect is not
```

Researcher
ANDREW MELLINGER

Next-Generation Battlefield Networking with FABRIC

In civilian life, we take for granted the connectivity that allows us to use our phones and computers to send messages, stream videos, and attend virtual meetings—often while moving from place to place and from network to network.

"On a battlefield, you don't have this luxury," said Andrew Mellinger, team lead for the SEI's work on the Future Autonomous Battlespace RF with Integrated Communications (FABRIC) project. The SEI team is helping to develop a next-generation wireless mesh network for battlefields.

Legacy systems make the connectivity civilians take for granted difficult to bring to the battlefield: these systems have grown over time and were not designed to work together. For example, soldiers on the ground may be using different equipment and networks than air support.

Untapped hardware capabilities also play a part. "To some degree, the networks have not changed to keep up with the changes and speed of the technology," explained Mellinger. "Hardware has gotten faster, and the corresponding software hasn't taken advantage of that."

The FABRIC project as a whole is developing a new set of radio hardware. The SEI's role is on the software side of things, working with an array of collaborators from other universities and FFRDCs to create a peer-to-peer, IP-based, wireless mesh network on which each device acts as a router and endpoint.

Mellinger pointed out that much of this effort draws on the SEI's role as a trusted advisor: "We are helping stakeholders understand how this technology is going to be used and make it useful in their mission space."

> *"To some degree, the networks have not changed to keep up with the changes and speed of the technology. Hardware has gotten faster, and the corresponding software hasn't taken advantage of that."*
>
> **—ANDREW MELLINGER, SENIOR SOFTWARE DEVELOPER**

Photo: U.S. Air Force

Researchers
ART MANION, SUMMER FOWLER

SEI Staff Offer Expert Testimony to Senate and House Committees

In 2018, SEI staff provided expert testimony on two issues of concern to the U.S. government: coordinated vulnerability disclosure (CVD) and the government's cybersecurity risk profile.

In July 2018, Art Manion, vulnerability analysis technical manager in the SEI's CERT Coordination Center (CERT/CC), testified before the U.S. Senate Committee on Commerce, Science, and Transportation in a hearing titled "Complex Cybersecurity Vulnerabilities: Lessons Learned from Spectre and Meltdown." These vulnerabilities affected features in modern CPU hardware designed to improve performance, and they carried serious implications for several areas of concern in CVD.

The hearing specifically examined complex CVD practices and supply chain cybersecurity in such cases, and how best to coordinate cybersecurity efforts going forward. For instance, Spectre and Meltdown raised the question of whether CVD practices are tuned too far in favor of preventing premature public disclosure. Manion outlined the specific challenges these vulnerabilities presented to CVD and offered a number of considerations to take into account for tuning CVD guidance.

"Meltdown and Spectre set an inflection point in the history of CVD and Internet security," Manion noted in his testimony. "The researchers and, more importantly, the coordinating vendors, could have recognized the need to at least reduce surprise by informing the U.S. government (and possibly other governments) sooner. Such a decision is already accounted for in existing CVD guidance; implementing it is a matter of tuning for known parameters."

> *"Meltdown and Spectre set an inflection point in the history of CVD and Internet security."*
>
> **—ART MANION, VULNERABILITY ANALYSIS TECHNICAL MANAGER**

Ultimately, according to Manion, effective CVD management comes down to the people involved in the process.

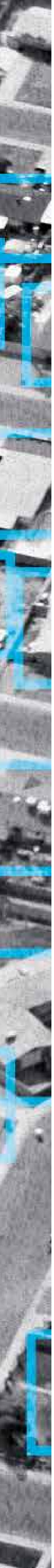
"CVD is a process of coordinating human behaviors," said Manion in his summation. "Success at multiparty coordinated vulnerability disclosure has more to do with understanding human communication and organization phenomena than with the technical details of the vulnerability."

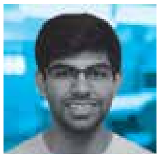
Also in July of 2018, Summer Fowler, then technical director of risk and resilience in the SEI's CERT Division, testified before the U.S. House of Representatives Cybersecurity and Infrastructure Protection Subcommittee of the Homeland Security Committee. The hearing, "Assessing the State of Federal Cybersecurity Risk Determination," used the May 2018 Office of Management and Budget (OMB) and Department of Homeland Security report titled "Federal Cybersecurity Risk Determination Report and Action Plan" as a point of departure and guide to understanding enterprise-wide cybersecurity risks and how the government is addressing them.

Fowler lauded the OMB report but noted it did not take into account the potential impact of cybersecurity risks. "If agencies are to achieve the ability to complete their mission no matter the cyber threat," noted Fowler, "it is imperative they manage both the cyber threat and the consequences of the attack [....] Accomplishing this continuity of operations requires a resilience approach to cybersecurity—an integrated, holistic way to manage security risks, business continuity, disaster recovery, and IT operations executed in the context of each organization's mission and strategy."

> For more information about the testimony of Manion and Fowler at these hearings, visit **resources.sei.cmu.edu** and search for "2018 SEI Year in Review Resources."

Photos: U.S. Customs and Border Protection, Architect of the Capitol





Researcher
RITWIK GUPTA

Speeding Up Satellite Image Analysis with Machine Learning

Overhead imagery is a powerful resource for mapping; monitoring the environment; information, surveillance, and reconnaissance (ISR); and much more. Yet it's possible to have too much of a good thing. The vast size of these image data sets makes them time-consuming to analyze. While machine vision can automate this task, it cannot always identify objects on the ground quickly and reliably.

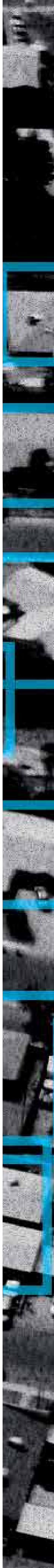
> *"Making sense of satellite imagery can be an enormous challenge."*
>
> **—RITWIK GUPTA, MACHINE LEARNING RESEARCHER**

"Making sense of satellite imagery can be an enormous challenge, especially when the area involved is large, time is of the essence, and the objects populating that area are many and diverse," said Ritwik Gupta, a machine learning researcher at the SEI's Emerging Technology Center (ETC).

In 2018, Gupta and his team of ETC interns, 2nd Lt. Alex Fulton (a graduate student at the U.S. Air Force Institute of Technology and Carnegie Mellon's Information Networking Institute) and Kaylene Stocking (an undergraduate student at the University of Pittsburgh) developed simple, innovative techniques for accurately localizing and classifying objects in overhead imagery. Their solution was strong enough to place in the top five entries at the 2018 Defense Innovation Unit Experimental (DIUx) xView Detection Challenge.

One of the techniques Gupta's team applied was an overlapping adaptive "chipping" strategy to overcome the xView data set's large size and object density. It divided images into overlapping squares, or chips, that intersected by a factor that depended on the density of objects within each chip. Their machine learning algorithm used the results from overlapping chips to localize objects within each chip faster and more accurately.

"This method can speed up real-world analysis of very large satellite images," said Gupta. Its applications include natural disaster response, mission planning, and any other situation where time and accuracy are critical. This innovative technique is just one example of the ways in which the SEI is working to maintain the DoD's information advantage.



Researcher
GRACE LEWIS

Bringing High-Assurance, Software-Defined IoT Security to the DoD

Internet of Things (IoT) technology is rapidly evolving, and the DoD understands the need to embrace it to keep pace with its adversaries. In fact, the DoD already uses IoT devices for resource management in its SCADA systems, and it's eyeing the use of IoT in tactical systems for surveillance, reconnaissance, and military intelligence. But untrusted supply chains and other security concerns have made the DoD reluctant to fully adopt IoT technology.

The DoD's caution is understandable. "IoT devices are typically exposed to potentially serious threats," said SEI researcher Grace Lewis. "These devices can be exploited to gain access to data, change data, send data to unauthorized systems, and even change firewall settings."

Lewis is collaborating with CyLab researcher Vyas Sekar and Carnegie Mellon University PhD student Capt. Matt McCormack to reduce or eliminate these concerns.

One facet of their project employs software-defined networking (SDN) and network function virtualization (NFV) to create a highly dynamic IoT security infrastructure. This approach tunnels traffic to and from IoT devices through µmboxes in the data plane that implement the desired network defense for the device. (µmboxes, or micro-middleboxes, are virtual machines or containers, such as firewalls, that implement the network defense for a specific IoT device.) An IoT controller residing in the control plane monitors the state of each device and alerts coming from µmboxes to determine whether, owing to a suspicious state or network traffic, a different µmbox must be deployed.

In addition, the researchers are delivering high assurance by using überSpark to incrementally develop and verify the security properties of elements of the software-defined IoT security infrastructure. überSpark is a framework used for building secure software stacks that

- are compatible with inexpensive devices that are widely available and interchangeable
- enable automated compositional verification of security properties
- produce systems that are fast, accurate, flexible and capable

> *"IoT devices are typically exposed to potentially serious threats."*
>
> **—GRACE LEWIS, PRINCIPAL RESEARCHER**

"The combination of these approaches migrates security enforcement to the network," said Lewis. "This allows IoT devices to be integrated into DoD systems, even if the IoT devices themselves are not fully trusted or configurable."

Lewis and her collaborators will validate their approach using the following techniques:

- **threat modeling** to identify, enumerate, and prioritize threats from a hypothetical attacker's point of view
- **policy abstractions** to account for the security status of IoT devices, alerts from network monitors, environmental conditions, and the state of the network devices
- **validation** to conduct model-based testing to ensure compliance, active testing to ensure that the network correctly implements the intended security posture, and static verification of policies to avoid conflicts and implicit threats

This work is in its early phases, but the team plans to demonstrate results by developing an end-to-end prototype. "We want to create a software-defined IoT security framework that operates in a resilient, trustworthy manner even in the presence of a powerful and realistic attacker who can compromise IoT devices," said Lewis.

> To learn more about this and other topics discussed in the *Year in Review,* visit **resources.sei.cmu.edu** and search for "2018 SEI Year in Review Resources."

Photos: U.S. Air Force, U.S. Navy, U.S. Army

Researcher
BJORN ANDERSSON

New SEI Method Verifies Timing in Undocumented Multicore Processors

Many Department of Defense (DoD) systems rely on multicore processors. These processors share resources and perform complex operations that depend on accurate timing and sequencing. This timing is crucial to ensuring proper and safe operation of the overall system, but verifying multicore processor timing can be a tricky and difficult business, especially when key details, such as processor resource sharing, often go undocumented. An SEI project led by researcher Bjorn Andersson has made strides in getting a handle on this important challenge.

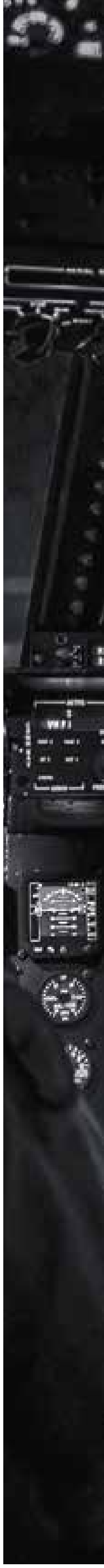
Multicore processors—computers with many processor cores running programs simultaneously—are employed to achieve more computing power with lower power consumption, smaller size, and higher reliability. The DoD often employs them in embedded systems as part of larger systems, where they are subject to real-time constraints on timing from event to system response. For example, in an aircraft, countermeasures must deploy not only correctly but at the right time.

Because multicores share resources, such as memory caches and buses, timing verification must consider the delays that a program can experience as a result of sharing resources. Verifying timing guarantees in mission- and safety-critical systems is so difficult that practitioners often disable all but one processor core, making multicores behave like single-core processors and sacrificing their benefits for easier verifiability. Such practices are not optimal.

"Verifying timing guarantees for shared resources is challenging for several reasons," said Andersson. "The number of possible schedules is too large to manually check each one. We need a verification technique that proves correct timing without enumerating all possible schedules." Such verification requires a model of both the software and the hardware; the latter requires documentation of which hardware resources exist and how they are shared.

Unfortunately, for many hardware resources, this information is not publicly available, and developers have to make assumptions about how shared hardware resources work. Even where documentation exists, technology evolves quickly, and a software system verified on today's hardware may not function the same on future hardware. Should the industry put even more effort into modeling every resource and interaction as operations grow ever more complex? "It's hard to model everything," said Andersson, "and then things change."

To address this challenge, Andersson led the SEI's Timing Verification of Undocumented Multicore project to develop a method for verifying the timing of software executing on multicores without information about shared hardware resources. Andersson, with external collaborators Hyoseung Kim (University of California, Riverside) and John Lehoczky (Carnegie Mellon University), developed a model that describes the *effect* that the execution of one program can have on the execution of another program. This model then becomes input to a tool that can prove that the overall software system has correct timing. Andersson explains, "Proofs always rely on assumptions. Our model is much closer to reality—this is the big selling point of our work."



By using a method like the SEI's timing verification for undocumented multicore, the DoD could field hardware upgrades more rapidly. The method decreases the amount of testing required when new components replace old ones in a system. Instead of creating a new model built on new assumptions to verify the system again, the upgrade effort would feed new numbers into the same descriptive model for faster results.

To learn more about this and other topics discussed in the *Year in Review,* visit **resources.sei.cmu.edu** and search for "2018 SEI Year in Review Resources."

Photo: U.S. Air Force

Researcher
NATHAN VANHOUDNOS

Using Artificial Intelligence to Find Security Defects in Code

“Think of code not as just a set of algorithms, but as a language—a method of communication between developers that runs on computers,” said Nathan VanHoudnos, a senior machine learning research scientist in the SEI’s CERT Divsion. “Static analysis tools ignore this semantic aspect of software. We want to use the natural language features of code to improve upon static analysis.”

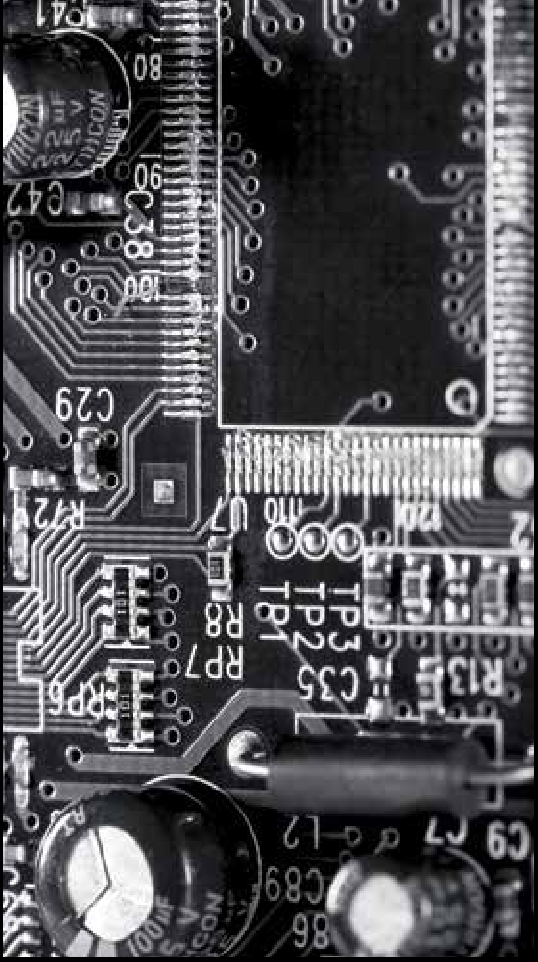
Static analysis tools are important because they’re widely used to find security defects in software. These tools analyze source code to see if it follows commonly accepted practices for developing safe, reliable, and secure systems. They use techniques like abstract modeling, data flow analysis, and model checking to identify security problems that are difficult to spot through other forms of testing.

Unfortunately, output from static analysis tools often includes false positives: innocuous code incorrectly identified as a security vulnerability. Software developers must investigate these warnings to see if they’re valid, and a high false-positive rate makes it harder to find and fix actual security vulnerabilities.

VanHoudnos believes artificial intelligence (AI) can cut through the clutter of false positives and do a better job of finding security vulnerabilities than static analysis tools. He’s building on pioneering SEI work begun by Carson Sestili and William Snavely to create a data-driven, machine-learning-based approach for finding security defects in source code.

To put their ideas to the test, VanHoudnos and a team of SEI colleagues are training a neural network to learn which lines of C code represent safe or unsafe coding practices. They began with a common security defect in C code: the buffer overflow. The C coding language permits programs to write values to a buffer outside of its defined boundaries, causing the buffer to overwrite adjacent memory. Hackers can exploit this vulnerability to inject malicious code, destroy data, and cause systems to behave erratically or crash.

The team generated a dataset using a tool it created called *sa-bAbI*. The *sa-bAbI* generator can produce a large number of code samples at a level of complexity that’s controlled by the user. The dataset produced by the team included both safe lines of C code and unsafe lines vulnerable to buffer overflow. The team then used neural network-based natural language processing to analyze the training dataset and



semantically identify which lines of code cause buffer overflow.

The team's proof of concept was a success. While the neural network's performance approached that of the best static analysis tools, the training time was long. But this proof of concept demonstrated that a machine-learning-based approach is feasible. VanHoudnos is planning to shorten the training time by applying deep learning algorithms that can perform arithmetic operations and including more expressive representations of source code in training data.

To spur further research in this area, VanHoudnos released *sa-bAbI* to the National Institute of Standards and Technology (NIST), which is incorporating it into the Software Assurance Reference Dataset (SARD). This will give programmers, researchers, and tool developers the ability to generate code with a known security flaw.

"We need to be able to write trustworthy software without security vulnerabilities," VanHoudnos said. "This project shows that AI has the potential to complement or even eventually replace static code analysis, which has broad implications for improving software assurance."

> *"This project shows that AI has the potential to complement or even eventually replace static code analysis, which has broad implications for improving software assurance."*
>
> **—NATHAN VANHOUDNOS, SENIOR MACHINE LEARNING RESEARCH SCIENTIST**

Photos: U.S. Navy

013

Researcher
JARED ETTINGER

Collaboration with ODNI Seeks to Improve the Practice of Cyber Intelligence Nationwide

What can we learn about cyber intelligence from high-performing organizations? Over the past year, the SEI has conducted interviews with companies and organizations all over the country to answer this and other questions. The interviews are part of a cyber intelligence study sponsored by the U.S. Office of the Director of National Intelligence (ODNI). The study will provide a snapshot of the state of the practice of cyber intelligence as well as actionable steps organizations can take to achieve high performance.

At the end of fiscal year 2018, the SEI was wrapping up interviews with 32 organizations representing critical infrastructure sectors ranging from banking to government to healthcare. "We're seeing a lot of common best practices among high-performing organizations, and we're finding shared challenges in areas where organizations struggle," said Jared Ettinger, a cyber intelligence researcher with the SEI Emerging Technology Center and the study's lead. "We're distilling our findings into recommendations that can improve how cyber intelligence teams all over the country do their work."

This study is a follow-up to a 2013 study of cyber intelligence practices. It examines these practices in five areas the SEI has defined as foundational to cyber intelligence:

- understanding your environment
- gathering data
- functional analysis
- strategic analysis
- decision maker reporting and feedback

Ettinger and his team ask participating organizations to describe how they perform a variety of tasks related to each of the areas, and to list resources such as tools and frameworks they find helpful. The SEI will release a public report of its findings in May 2019.

To learn more about this and other topics discussed in the *Year in Review,* visit **resources.sei.cmu.edu** and search for "2018 SEI Year in Review Resources."

"We're seeing a lot of common best practices among high-performing organizations, and we're finding shared challenges in areas where organizations struggle."

—JARED ETTINGER, CYBER INTELLIGENCE ANALYST

Researchers
OREN WRIGHT, DANIEL JUSTICE, AND WILL BOLER

Training Machines to Recognize Emotions in the Human Voice

Accurately recognizing and identifying emotions in the human voice holds great potential for defense applications, healthcare, intelligence, and law enforcement. Future human-machine teaming scenarios will depend, in part, on the ability of machines to understand and react to expressions of human emotions. Because the human voice contains traces of many bio-parameters, including emotional state, the SEI's Oren Wright is leading an effort with SEI colleagues Daniel Justice and Will Boler to create techniques to teach machines how to recognize emotions in human voice in the same way we do.

Wright's work builds on previous SEI initiatives to reveal emotions from facial micro-expressions and heart rate extracted from video, but it differs in two important ways. First, it employs micro-articulometry, a tool advanced by Wright's collaborator on this project, Rita Singh at Carnegie Mellon University (CMU).

Micro-articulometry analyzes voice features at the phoneme level (the smallest unit of speech) to create a measurement of high-resolution, fine-grained characteristics. Singh, who works at the CMU Language Technologies Institute, has applied micro-articulometry to voice forensics on more than 50 criminal cases for which voice recordings were the only evidence.

According to the researchers, analysis at this level has several advantages. Phoneme-level signatures, often undetectable at the utterance level, can be found in voice qualities such as jitter (roughness of pitch due to frequency variation) and shimmer (crackle due to short-term amplitude variations). The researchers are looking for fine changes in voice features that allow us to then estimate bio-parameters, like emotional state.

The second new aspect of this research is the use of PAD, an emotional-state model borrowed from the field of psychology. The PAD model allows measurement of emotions or affects in the dimensions of pleasure, arousal, and dominance in a continuum rather than as discrete labels, as is commonly the case in current speech-emotion databases.

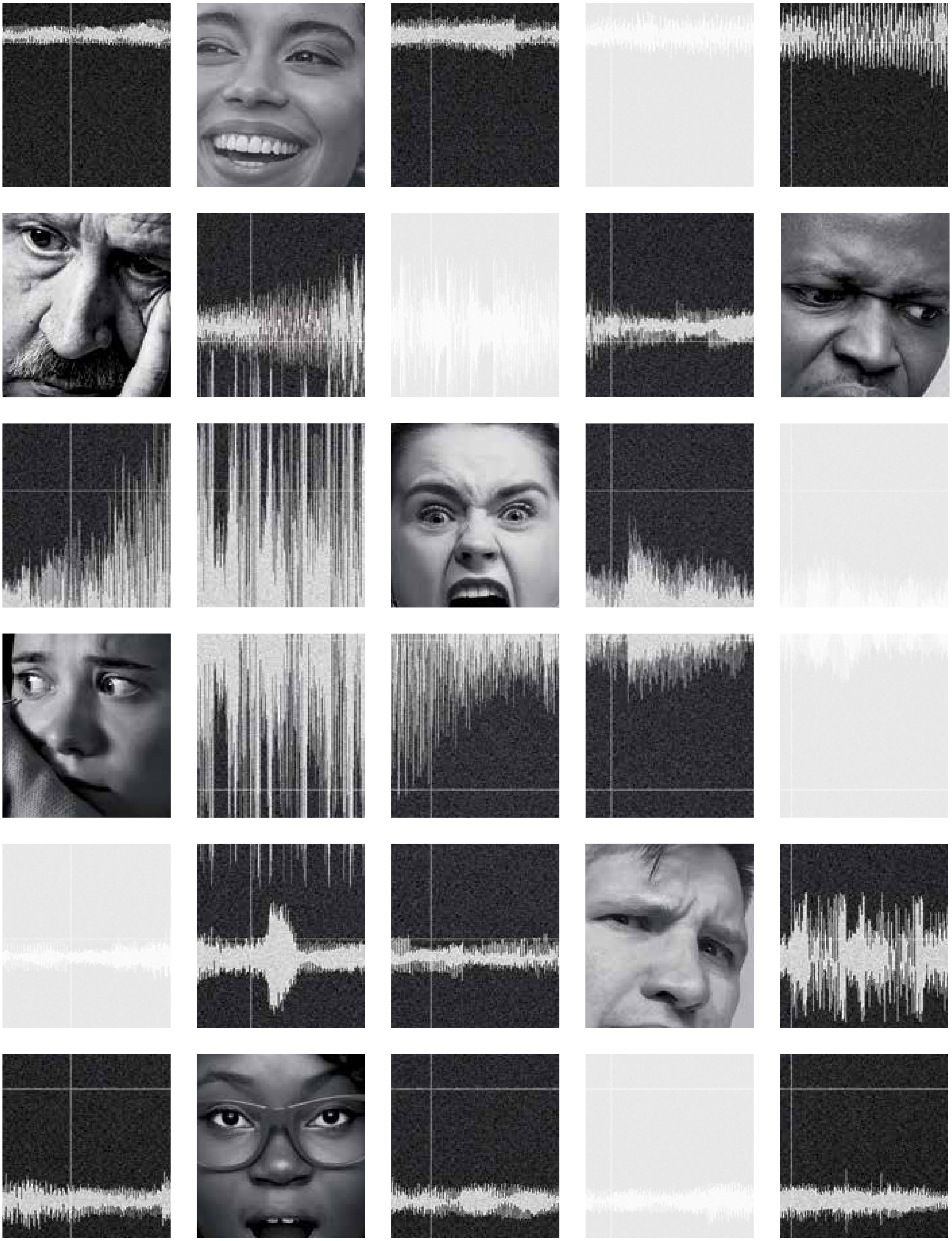
The team is designing and implementing machine-learning systems that use a robust, continuous emotional-speech database based on PAD and a set of well-developed micro-articulometry techniques. Together these innovations allow for the creation of an emotion-recognition prototype with the potential to be applied to practical missions.

Wright is currently focused on three tasks:

- creating a new voice database that maps to a continuum of emotions
- extracting of micro-features
- designing and training machine-learning algorithms to estimate emotional status from those micro-features

According to the researchers, computers are now outperforming people at object recognition. Their hope is that their work will pave the way for machines to one day perceive emotion with such accuracy and granularity that they will exceed human capabilities. This will allow machines to become more empathetic and intelligent when interacting with and supporting their human teammates and counterparts.

> To learn more about this and other topics discussed in the *Year in Review,* visit **resources.sei.cmu.edu** and search for “2018 SEI Year in Review Resources.”



SPACECOM-05
FLIGHT OPERATIONS
ITL TO DEEP SPACE NETWORK TO MCC
END TO END COMPATIBILITY TEST
ECOM
FLIGHT
GNC

Researcher
WILL HAYES

SEI Gives NASA IV&V Team an Agile Boost

It's named Orion: the first new human-crewed spacecraft developed by NASA since the Space Shuttle. For the past two years, the SEI has helped Orion's Independent Verification and Validation (IV&V) team learn and adopt Agile, a modern, user-value-centered development process increasingly used by commercial software development teams.

"Two years ago, the Orion IV&V team was struggling," said NASA's Justin Smith, the team's project manager. "We were struggling to provide software assurance to a NASA project that was being developed through an Agile development model."

That's when NASA requested the SEI's help. The institute is home to considerable knowledge and expertise in helping U.S. government programs learn and implement the iterative and incremental approaches commonly known as "Agile."

Will Hayes of the SEI's Client Technical Solutions team led the knowledge transfer effort—and, according to Smith, made a difference from the start.

"We initially hired Will to help our team understand how the developer was using Agile," Smith said. But the SEI team didn't stop there, Smith said, noting that Hayes "learned about the IV&V processes [and] was able to start to put some pieces together."

The result? Agile IV&V—the application of those relevant Agile and Lean principles in the planning, management, and performance of IV&V.

The team embraced the continuous improvement mindset, and Orion IV&V changed delivery cadence from months to weeks. Stakeholders in the Orion program took note of the changes, with one saying, "IV&V's capability-based approach and 'follow the risk' strategy allows [team members] to have relevant opinions on the most difficult issues the program is facing. Their recommendations and conclusions are well researched and obviously vetted internally. They consistently bring coherent communication and clarity to discussion, and I highly value their opinion."

Smith's team continues to work with Hayes and others at the SEI. "It's really been a great experience for me—and the whole SEI Agile team—to work with NASA's Orion IV&V group," Hayes said. "They were very courageous and very professional in embracing and integrating Agile principles into their Capability Based Assurance approach."

Photos: NASA

Researchers
ALEXIS PRESTI-SIMPSON, SCOTT HISSAM, ANNIE DRAZBA, AND ANDREA LEIGH AMRAM

SEI Staff Strengthen Working Relationships Across the Country

To increase the SEI's impact for the DoD, the SEI supports a number of staff members who are strategically located near emergent and growing customers. In addition to previously placed staff in Colorado, Florida, and other areas, the SEI now has staff members located in Boston, Massachusetts; Los Angeles, California; Patuxent River, Maryland; and San Antonio, Texas. This close proximity to sponsor organizations helps better align the SEI's research with the DoD's strategic needs and also enables the DoD to take better advantage of the SEI's research and expertise.

Alexis Presti-Simpson leads the Boston area team, the SEI's largest outside of Pittsburgh and Arlington, which supports the Program Executive Officer (PEO) for Command, Control, Communication, Intelligence, and Networks; the Digital PEO; the Nuclear Command, Control, and Communications (NC3) PEO; the Cyber Resilience of Weapons Systems (CROWS) office; the 96th Cyber Test Group and Defense Innovation Unit (DIU); and Kessel Run Experimentation Lab (KREL). All of these units operate out of Hanscom Air Force Base in the Boston area.

"The leadership at Hanscom appreciates having the SEI on location as an extended part of their team," said Presti-Simpson. "They can interact with SEI staff directly and quickly get answers to questions about high-value efforts within their portfolio."

Presti-Simpson noted that for each PEO, the SEI supports a number of technical research and development programs. These programs involve areas such as open mission systems research and development, network analysis, technical threat analysis, mission thread analysis, big data analysis, and training. "We continue to see a high demand for our expertise as systems become increasingly software dependent," said Presti-Simpson. "The SEI team in Boston will be here to grow with and meet that demand."

In San Antonio, Scott Hissam heads up a team supporting the U.S. Air Force Lifecycle Management Center, specifically its Human Resources Systems (AFLCMC/HIH) and Cryptologic and Cyber Systems (AFLCMC/HNC) divisions. Their work includes acquisition support, risk assessment, and process improvement.

"Establishing the local relationship had an immediate impact with AFLCMC/HNC's location at JBSA-Lackland," said Hissam. "Their leadership saw an opportunity to get ready access to SEI's experience and expertise in software and cyber engineering, not by picking up the phone but by walking across the hall or to the next cubicle."

This proximity has been mutually beneficial. "Our presence not only gives our partners instant access to advice, consultation, and feedback," noted Hissam, "but it often results in conversations that enlighten our partners to possibilities for advanced software engineering techniques, which may have gone undiscussed in a non-face-to-face engagement."

In Patuxent River, Annie Drazba leads a team supporting the Naval Air Systems Command (NAVAIR), which is located at Patuxent Naval Air Station. NAVAIR's mission is to provide full lifecycle support for naval aviation aircraft and weapons and systems operated by sailors and Marines. Drazba's team supports NAVAIR in different phases of the software acquisition and development

lifecycles. It also applies research in support of NAVAIR Science and Technology programs.

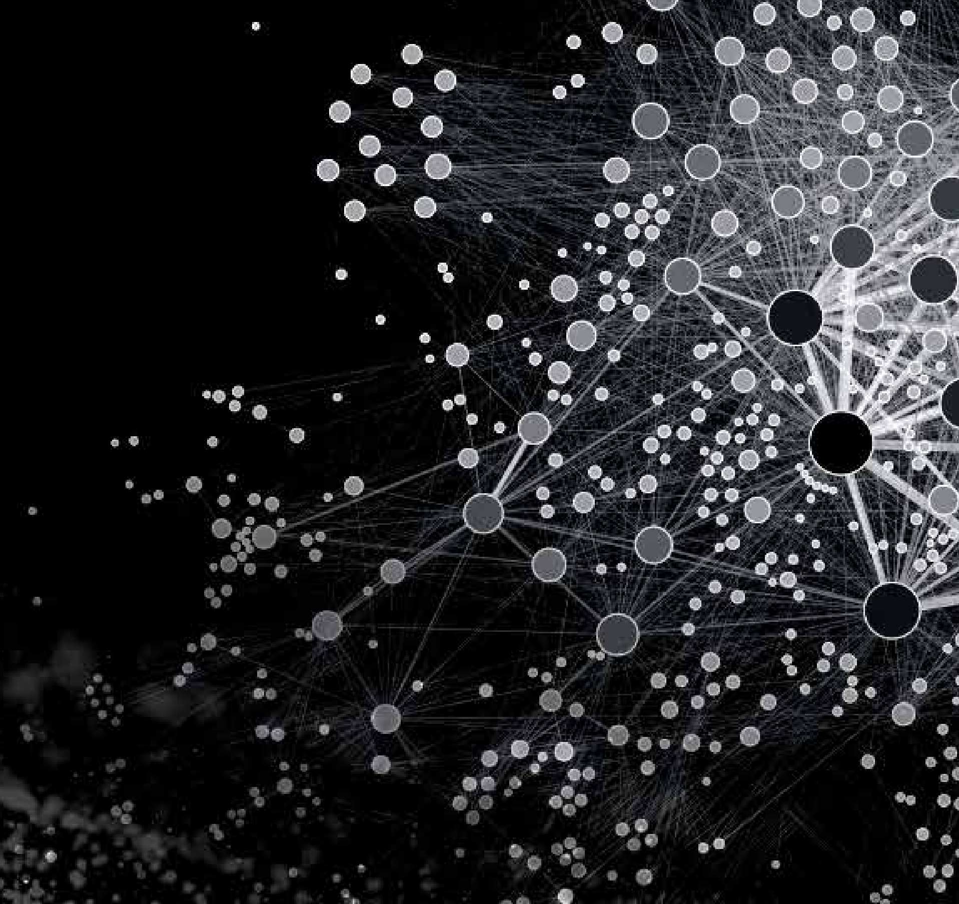
Drazba cited a number of advantages to having a presence in Patuxent River. “We are very accessible to our customers,” she noted, “and being here allows them an off-base opportunity to meet with us. Also, we’re close to other industry, academia, and DoD partners, allowing for collaboration opportunities. As members of the Patuxent Partnership, the SEI has a seat at the table to advance science and technology initiatives through an exchange of ideas.”

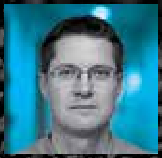
Andrea Leigh Amram heads up the team in Los Angeles that supports the Air Force Space and Missile Systems Center (SMC) in Los Angeles and its broader program organizations in Boulder, Denver, and Colorado Springs, Colorado, and Albuquerque, New Mexico.

“In the last two years, we’ve worked to establish the SEI as the software and cyber FFRDC at the SMC,” said Amram. “Currently, we’re focused on the front end of programs pursuing prototyping, DevOps, and Agile approaches to ground system development and embedded systems secure code analyses.”

All the SEI teams around the country are working hard to support the important missions of our sponsors, establishing close working relationships that help the SEI better understand the organizations we serve and the challenges they face.

Photos: U.S. Navy, U.S. Air Force, U.S. Air Force: Airman 1st Class Stormy D. Archer





Researcher
SCOTT MCMILLAN

Unlocking the Potential of Next-Generation Hardware

The fabric of computing is changing. In the quest for better performance, new hardware architectures are being introduced constantly. Multi-core central processing units (CPUs) have become standard. What's more, the use of multiple CPUs, heterogeneous systems with graphic processing units, field-programmable gate arrays, and application-specific integrated circuits (ASIC) are also becoming commonplace. Although such systems offer massive processing and power consumption advantages, software engineering challenges often put those advantages out of reach: the hardware is different and too complicated to program efficiently.

This is why the SEI is working to enable software developers and engineers to take full advantage of these challenging technologies. Scott McMillan, a research scientist with the SEI's Emerging Technology Center, leads a portfolio of work in advanced computing that has been building over the past five years.

One area of McMillan's work involves Graph Basic Linear Algebra Subprograms (GraphBLAS), a programming specification for graph analysis. Graph algorithms are in wide use in DoD software applications, but despite their utility and wide use, graph algorithms are difficult and costly to implement. What's more, they're hardware dependent, and the complexity of developing high-performance graph libraries is becoming a barrier to analyzing the deluge of information. McMillan, in a pioneering collaboration with the GraphBLAS Forum and collaborators from government, universities, and industry, released an application programming interface (API) specification that separates the concerns of graph algorithm writers who would use the primitive (building block) GraphBLAS operations from those of GraphBLAS library users whose main concern is to implement the fastest possible primitives for the hardware they target.

"If we achieve a separation of these concerns—where graph experts can program their applications using higher-level math abstractions and leverage another team's hardware expertise—we can develop software for high-performance graph libraries

much more easily," said McMillan. "Our work reinforced the overall mission of the GraphBLAS Forum: to allow graph experts to write once, run everywhere, and run fast."

McMillan's team, along with GraphBLAS collaborators, also developed a test framework for the API. Developers can use the test framework to verify that their libraries are performing correctly.

Even with this separation of concerns, the effort and expertise needed to implement fast primitives remain great. The team turned to automatic code generation to allow computers to derive the best implementations of those primitives. Using formal specifications of hardware capabilities, Carnegie Mellon University's Spiral code generation technology can already automatically generate high-performance signal-processing codes. Working with the Spiral project's leaders and team members at Carnegie Mellon, the SEI team is expanding Spiral's automated code generation technology to use mathematical formalization of the GraphBLAS primitives to automatically generate the high-performance graph applications needed for targeted hardware platforms.

The GraphBLAS API is also finding use in domains beyond graphs: machine learning and artificial intelligence. The team will be expanding on this research to explore implementations of artificial intelligence/machine learning algorithms using GraphBLAS as well as expanding Spiral's capabilities in this direction.

The team also plans to enhance the automatic code generation system developed with Spiral to select appropriate hardware: based on constraints like cost, size, weight, and power, the system will select the appropriate hardware from available COTS components, all while generating high-performance code for the selected hardware. This process, referred to as ***hardware-software co-optimization***, is the next step to achieving the ultimate goal of co-synthesis in which the hardware would be completely designed.

CMU Leadership

Farnam Jahanian
President

James H. Garrett, Jr.
Provost and Chief Academic Officer

J. Michael McQuade
Vice President, Research

SEI Executive Leadership

From left to right:

Tom Longstaff, Chief Technology Officer; Paul Nielsen, Director & Chief Executive Officer; David Thompson, Interim Deputy Director and COO

SEI Technical Directors

From left to right:

Matt Gaston, Director, Emerging Technology Center; Bobbie Stempfley, Director, CERT Division; Anita Carleton, Interim Director, Software Solutions Division

SEI Functional Directors

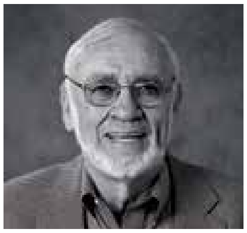
From left to right:

Dan Bauer, Director, Talent Management; Sandra Brown, SEI General Counsel; Mary Catherine Ward, Chief Strategy Officer; Heidi Magnelia, Chief Financial Officer; John Bramer, Chief of Staff

Board of Visitors

The SEI Board of Visitors advises the Carnegie Mellon University president and provost and the SEI director on SEI plans and operations. The board monitors SEI activities, provides reports to the president and provost, and makes recommendations for improvement.

Barry W. Boehm
TRW Professor of Software Engineering, University of Southern California; Director, University of Southern California Center for Software Engineering



Gilbert F. Decker
Consultant; former President and CEO, Penn Central Federal Systems Company; former President and CEO of Acurex Corporation; former Assistant Secretary of the Army/Research, Development, and Acquisition

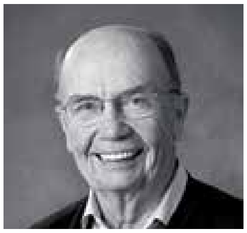
Philip Dowd
Private Investor; former Senior Vice President, SunGard Data Systems; Trustee, Carnegie Mellon University

John M. Gilligan
President, Gilligan Group; former Senior Vice President and Director, Defense Sector of SRA International; former CIO for the Department of Energy

Elizabeth A. Hight
Former Vice President of the Cybersecurity Solutions Group, Hewlett Packard Enterprise Services; former Rear Admiral, U.S. Navy; former Vice Director of the Defense Information Systems Agency

Tom Love
Chief Executive Officer, ShouldersCorp; Founder of Object Technology Group within IBM Consulting

Alan J. McLaughlin
Chair, Board of Visitors; Consultant; Former Assistant Director, MIT Lincoln Laboratory



Donald Stitzenberg
President, CBA Associates; Trustee, Carnegie Mellon University; former Executive Director of Clinical Biostatistics at Merck; Member, New Jersey Bar Association

SEI Leadership

DIRECTOR'S OFFICE

Paul D. Nielsen
Director & Chief Executive Officer

Tom Longstaff
Chief Technology Officer

David Thompson
Interim Deputy Director and COO

SOFTWARE SOLUTIONS DIVISION

Anita Carleton
Interim Director

John E. Robert
Deputy Director (Acting)

Charles Holland
Chief Scientist

EMERGING TECHNOLOGY CENTER

Matt Gaston
Director

Brenda Penderville
Deputy Director (Acting)

CERT DIVISION

Bobbie Stempfley
Director

Bill Wilson
Deputy Director

Greg Shannon
Chief Scientist

OFFICES OF THE COS/CIO

John Bramer
Chief of Staff

David Thompson
Chief Information Officer

FINANCIAL & BUS. SERVICES

Heidi Magnelia
Chief Financial Officer

STRATEGIC INITIATIVES

Mary Catherine Ward
Chief Strategy Officer

TALENT MANAGEMENT

Dan Bauer
Director

SEI LEGAL

Sandra Brown
SEI General Counsel

Copyright

Copyright 2019 Carnegie Mellon University. All Rights Reserved.

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Internal use:* Permission to reproduce this material and to prepare derivative works from this material for internal use is granted, provided the copyright and "No Warranty" statements are included with all reproductions and derivative works.

External use:* This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other external and/or commercial use. Requests for permission should be directed to the Software Engineering Institute at **permission@sei.cmu.edu**.

* These restrictions do not apply to U.S. government entities.

Carnegie Mellon®, CERT® and CERT Coordination Center® are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

DM19-0397

Credits

Manager, Communication Services
William Thomas

Manager, Corporate & Technical Communications
Janet Rex

Manager, Public Relations
Richard Lynch

Manager, Communication Design
Cat Zaccardi

Editor-in-Chief
Ed Desautels

Editorial
Hollen Barmer
Heidi Brayer
Ed Desautels
Tamara Marshall-Keim
Gerald Miller
Nancy Ott
Sandy Shrum
William Thomas
Barbara White

Design
Christopher Baum

Illustration
Kurt Hess

Digital Production
Mike Duda

Photography
David Biber
Tim Kaulen, CMU

20
18

SEI Pittsburgh, PA
4500 Fifth Avenue
Pittsburgh, PA 15213-2612

SEI Washington, DC
Suite 200
4301 Wilson Boulevard
Arlington, VA 22203

SEI Boston, MA
10 Maguire Road
Lexington, MA 02421

SEI Los Angeles, CA
2401 East El Segundo Boulevard
El Segundo, CA 90245

SEI Patuxent River, MD
Beck Building
23076 Three Notch Road
California, MD 20619