Carnegie Mellon University
Software Engineering Institute

2017
YEAR IN REVIEW

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 2017 SEI Year in Review highlights the work of the institute undertaken during the fiscal year spanning October 1, 2016, to September 30, 2017.

A MESSAGE FROM THE

Director and Chief Executive Officer

Without question, our national defense and security organizations know the threats our nation faces from adversaries across all operational domains, including cyberspace. The Defense Science Board's 2017 report on priorities, *Seven Defense Priorities for the New Administration*, for instance, spells out danger from enemy states, non-state actors, and others against U.S. armed forces and our information infrastructure.

Consequently, those organizations also are aware that software quality is more important than ever to mission success and sustaining information superiority. Our national defense and security organizations depend on complex, software-based technologies to identify threats, plan operations, conduct missions, arm warfighters, and train personnel. In addition, our weapon systems and the people who operate them are relying more and more on software-enabled autonomous systems.

Yet, in the Department of Defense (DoD) and elsewhere in the federal government, software development and sustainment organizations experience problems because of the sheer complexity of the software needed to deliver advanced capabilities. This complexity also drives quality concerns, vulnerability issues, and continuing cost concerns.

At the Carnegie Mellon University Software Engineering Institute (SEI), a DoD-sponsored federally funded research and development center (FFRDC), we develop software-based technologies to improve software quality by bending the software cost curve, reducing cyber risk by devising ways to eliminate software defects before they can be exploited as vulnerabilities, and building cyber workforce readiness.

In addition, we work to enable our sponsor and other government organizations to leap ahead technologically by realizing the potential of artificial intelligence and autonomous systems based on software that is resilient, assured, continually responsive to operational needs, and affordable.

More than ever, the DoD must negotiate a technology landscape dominated by software's expanding and deepening role in a dangerous world. To do so, the DoD—as well as the Defense Industrial Base, civil government, and industry—needs innovative technologies for software quality and security from its entire R&D network, especially the SEI.

Paul D. Nielsen
Director and CEO

A MESSAGE FROM THE

Chief Technology Officer

The intensely competitive technology environment supporting U.S. military capabilities requires the U.S. Department of Defense (DoD) to continually and rapidly develop and deploy innovative, software-enabled components and systems that are affordable, secure, resilient, and easy to modify. At the SEI, our technical work in the areas of software and cybersecurity promotes improved assurance of those software system qualities and behaviors, in particular those related to software cost and cyber vulnerability.

A significant portion of system lifecycle cost stems from finding and fixing software flaws only late in development. Studies have shown that efforts to fix software flaws late in the lifecycle, or after deployment, require much greater rework effort. Furthermore, flaws not addressed before a system is deployed can create cyber vulnerabilities that put missions and personnel at risk.

Our technical work strives to reduce software cost and cyber vulnerability; increase software producibility, capability, and speed; and address other persistent issues *early* in the system's development, when doing so is most effective. We develop data-driven, formally verified, and automated algorithms, tools, techniques, and practices to close critical technology gaps for those who defend our nation. We then deliver software-based capabilities through an execution model that combines our applied research and development, customer engagement, and deep expertise in transitioning solutions.

As a DoD-sponsored federally funded research and development center, we have a unique ability to undertake technical work ranging from fundamental research with widespread application to the support of sensitive government programs. We also serve as a value-added broker by working with software and cyber communities in government, academia (in particular, Carnegie Mellon University), and industry. In this role, we adapt innovative software and cybersecurity technologies that provide greater assurance of software-based systems for our sponsors.

Jeff Boleng
CTO (Acting) and Deputy CTO

Table of Contents

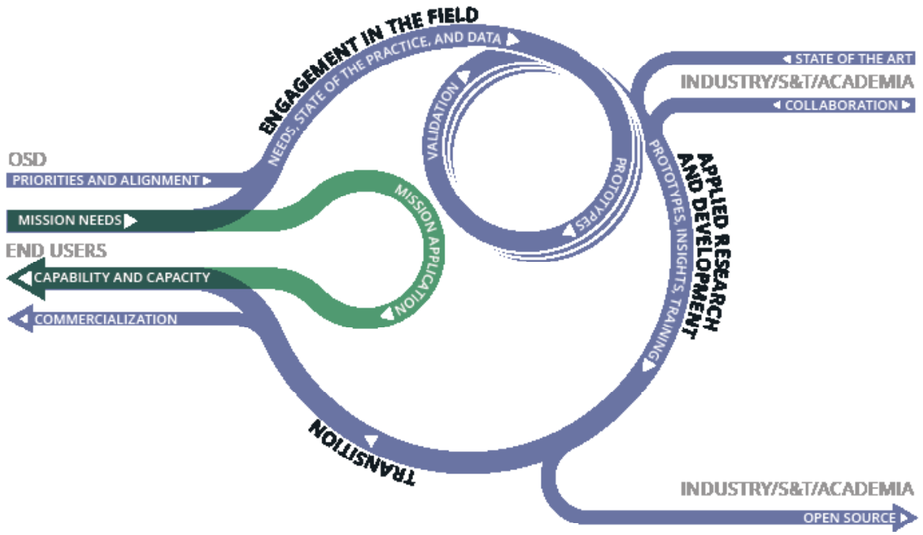
Execution Strategy

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 non-material 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. from t inform direct

U.S. Department of Defense (DoD) and other federal agencies, or agreements with non-federal 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.



FUNDING SOURCES

In FY 2017, the SEI received funding from a variety of sources in the Department of Defense, civil agencies, and industry.

Stempfley Takes the Reins as CERT Division Director

In June 2017, Bobbie Stempfley joined the SEI as director of the CERT Division. Stempfley succeeded SEI Fellow Richard Pethia, who led the unit since its inception in 1988. The CERT Division focuses on anticipating and solving the nation's cybersecurity challenges. It researches security vulnerabilities in software products, contributes to long-term changes in networked systems, and develops cutting-edge information and training to help improve cybersecurity.

"The CERT Division strives to make the smart decisions in cybersecurity the default decisions," noted Stempfley. "The field has a reputation for being difficult and confusing. Shifting this perception is an important part of a more resilient future and a more secure software ecosystem.

"We work to shift this paradigm by giving users, developers, and policymakers greater insight into the security consequences of decisions and indecision," said Stempfley. "For instance, understanding how to tie decisions made in development to risks that emerge in operations can be elusive. Our efforts in security-aware acquisition, secure development, and threat-aware sustainment are focused on helping in this area.

"We work to improve the state-of-the-art and the state-of-the-practice. We have a deep understanding of our customers' environments, emerging threats, and the evolving technology landscape. As a key partner to the federal government and its providers, we connect and evolve the research and its application. Each research opportunity and every customer engagement is about making that connection," Stempfley said.

Stempfley also noted that while the Department of Defense (DoD) and other organizations can become more agile as a result of software advances, they also can fall victim to security issues arising from the complexity that delivers them. "Our work is about exposing the risks associated with complexity in order to address them more fully and rapidly. For instance, our use of machine learning and data science helps agencies use automation to keep pace in their cyber monitoring and response operations with the changing environment surrounding them.

"Central to all our work is the development and implementation of measurable practices, which are essential to understanding how to balance the costs of complexity and the opportunities provided by software-fueled agility," Stempfley concluded.

SEI Collaborations Draw the Best and Brightest to Tough Software Engineering Challenges

The SEI's reach in the software engineering community, as well as its setting on the Carnegie Mellon University (CMU) campus, create ample opportunities to collaborate with thought leaders in a variety of fields on the tough software and cybersecurity challenges confronting the Department of Defense (DoD) and industry. In 2016, the SEI collaborated with researchers from CMU and other academic institutions, the DoD, other federally funded research and development centers, and the Agile Research Consortium. The challenges these collaborations addressed ranged from network defense to biometrics to self-healing code.

A number of these projects are highlighted in this edition of the *SEI Year in Review*. For example, the SEI's Andrew Mellinger has been involved in a multi-year project to create a reference implementation for an adaptive cyber defense platform for networks. Contributing to this important work on "moving target defense" is Marco Carvalho, a professor at the Florida Institute of Technology (FIT). Carvalho, a research scientist at FIT's Institute for Human and Machine Cognition and executive director of the Harris Institute for Assured Information, brings years of expertise in the areas of computer security, computer networks, and information systems.

Also contributing to this project are Professor David Garlan and principal research scientist bradley Schmerl, both of the Institute for Software Research (ISR) in Carnegie Mellon's School of Computer Science. Garlan and Schmerl are experts in self-adaptive systems. Together with Mellinger and Carvalho, Garlan and Schmerl are working to create the standard by which future dynamic network defense platforms can be evaluated, thereby laying the groundwork for meaningful research in this important area.

Satya Venneti, an SEI researcher specializing in machine emotional intelligence, heads up a project on real-time extraction of biometric data from video. The approach uses a hybrid of face landmarking techniques to achieve both speed and accuracy in natural settings. A key collaborator is Marios Savvides, director of the CyLab Biometrics Center at CMU. Savvides is an expert in the art of face landmarking. Venneti is also collaborating with Kris Kitani, assistant research professor in the Computer Vision Group of CMU's Robotics Institute. Kitani's work on human activity forecasting integrates optimal control and computer vision techniques in an effort to overcome the limitations of the traditional camera. The work of this collaborative effort holds potential in a wide range of scenarios, including security, surveillance, counter-terrorism, and identification.

The SEI's Will Klieber is leading an effort to advance the field of automated code repair. Joining Klieber is CMU professor Claire Le Goues, a leading researcher in the use of genetic programming for automated code repair. This work applies computational analogues of biological mutation and crossover to generate new program variants and to search for a variant that produces the desired result for all test cases. CMU's Christian Kästner, who has pioneered work on symbolically analyzing code under all possible build configurations, also contributed to this project, which seeks to develop a repair that works for all possible build configurations.

SEI researcher Lori Flynn is leading a team investigating the use of classification models to help analysts and programmers prioritize which vulnerabilities to address. Their goal is to reduce the effort required by software developers to triage the large number of potential code flaws typically identified by static analysis, which can hijack a software project's budget and schedule. Flynn's team has developed a prototype tool to classify alerts and prioritize some of them for manual analysis. The team is collaborating with three DoD organizations to field test their approach. Two of the collaborating organizations conducted static analysis of approximately 100 million source lines of code (SLOC) annually. Flynn's long-term goal is to develop an automated and accurate statistical classifier to much more efficiently target analyst effort and to remove code flaws.

These collaborative projects represent just a few of the ways in which the SEI engages in mutually beneficial collaborations. By teaming with experts at CMU and other institutions, the SEI advances the state-of-the-art and practice while tackling some of the toughest challenges facing the DoD and industry.

"We can turn future innovations into high-quality, affordable, and secure advanced capabilities for the DoD and others."

—MATTHEW GASTON, DIRECTOR, EMERGING TECHNOLOGY CENTER

Researchers
JEFF BOLENG, ROBERT STODDARD

Using Ground-Truth Data Sets as Engines of Innovation

Writing for *Defense AT&L*, Christian Hagen and Jeff Sorensen noted, "The capacity of the Department of Defense (DoD) and the military commands to defend our country will depend more on their ability to develop the best software rather than on the physical design chosen for the weapons. Like it or not, the DoD now is in the software business."

One way the SEI addresses DoD software quality concerns is by gathering and cultivating ground-truth data sets that serve as engines of innovation for software analysis tools. Examples of our applied research and development in FY17 illustrate how the SEI does this.

Drawing on its prior research and engagements with customer organizations, the SEI has gathered unclassified data sets into a software engineering data repository of detailed product and process data from 590 software projects and 4,200 software developers. The repository comprises data on software vulnerabilities, software cost, process improvement, and architecture evaluation. It also includes results from static code analyses for secure coding as well as technical assessments of IT and weapon systems.

"In wave after wave of software innovation, the availability of ground-truth data sets, possibly more than the formation of algorithms, has led to rapid advances," said Jeff Boleng, CTO (acting) and deputy CTO.

SEI researchers capitalize on this access to real-world data and research data to save time—because they do not need to recreate data for each new project—and expand their collaboration opportunities. For example, FY17 DoD-funded research used repository data to discover causal factors that drive software cost.

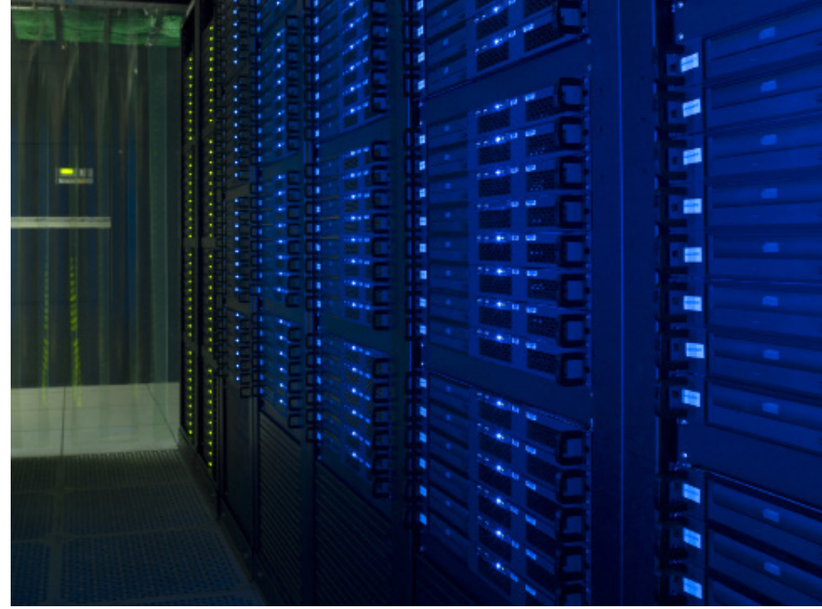
In this new work, a research team led by Robert Stoddard used new causal learning (CL) techniques to evaluate data sets representing about 60 unique cost factors and more than 15 cost relationships. The research put SEI-curated data sets at the disposal of an SEI technical staff expert in analytical tools and architectural analysis. Collaborating on the effort was Professor David Danks, a world-class expert in CL, of Carnegie Mellon University (CMU).

With these pieces in place, the SEI began a four-year journey to build an actionable, causal model of software cost and other acquisition outcomes. DoD programs and contract negotiators found the model useful. It provides new guidance on the application of causal discovery and inference algorithms to software engineering data. The model also meets the DoD need to identify the causes of high software costs, enabling new software policy and more informed negotiated pricing of contracted software.

Two other recent technologies related to DoD software cost also relied on data mining and curated data sets. The Quantifying Uncertainty in Early Lifecycle Cost Estimation method, developed with DoD funding, synthesizes scenario building, Bayesian Belief Network (BBN) modeling, and Monte Carlo simulation to depict influential relationships among program change drivers and outputs. The *DoD Software Factbook* provides analysis from the perspective of policy and management about software projects.

By applying new insights about software cost, architecture risk evaluation, code security, vulnerabilities, and other facets of software quality, DoD programs and federal agencies gain from the ground-truth data set based software technologies that the SEI develops, transfers, and broadly transitions. In turn, from engagement with those organizations, the SEI gains more high-quality data for its research.

> **To learn more** about this and other topics discussed in the Year in Review, visit resources.sei.cmu.edu and search for "2017 SEI Year in Review Resources."



Related Work

The use of curated ground-truth data sets as engines of innovation pervades SEI research. In addition to its software engineering data repository, other data sets informing new research include the following:

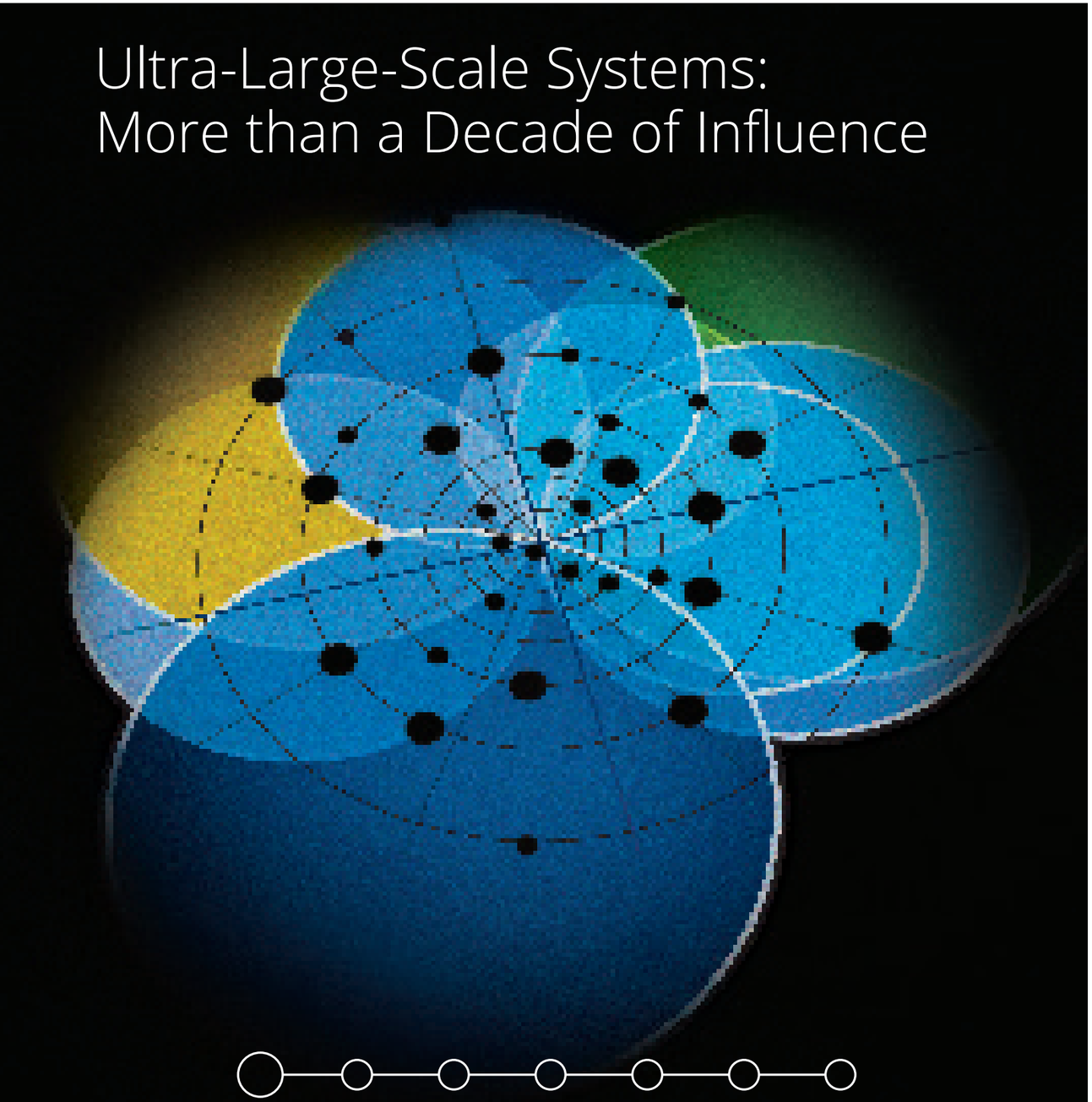
Malware Artifacts
For nearly 15 years, the SEI has been collecting malware samples in the CERT Artifact Catalog. Network situational awareness analysts, among others, extract indicators from the malware to discover malicious traffic on government networks.

Insider Threat Cases
Applying system dynamics modeling to its data set of more than 1,300 insider threat cases, SEI researchers characterize the nature of the insider threat problem, explore dynamic indicators of insider threat risk, and identify and experiment with administrative and technical controls for insider threat mitigation. Analysis of this data set produced the fifth edition of the *CERT Common Sense Guide to Mitigating Insider Threats*.

Photo: U.S. Department of Energy

SEI Fellow and Ultra-Large-Scale Systems Study Lead
LINDA NORTHROP

Ultra-Large-Scale Systems: More than a Decade of Influence



In 2005, the U.S. Army asked the SEI—the Department of Defense's (DoD) only federally funded research and development center focused on software—to convene a meeting of key influencers and thought leaders to envision future challenges in software engineering. In the wake of that meeting, the SEI led a follow-on team to produce the report *Ultra-Large Scale Systems: The Software Challenge of the Future*. That seminal report anticipated the characteristics of modern software systems and helped catalyze the foundational technology underlying those systems.

Motivating the Army's request was its drive to achieve information dominance in the field, best exemplified at the time by its effort to develop the Future Combat Systems platform. The Army recognized that software was the key to achieving this goal. However, as he noted in the SEI's 2005 report, Claude M. Bolton, Jr., then Assistant Secretary of the Army (Acquisition, Logistics, and Technology), saw challenges ahead. "Given the issues with today's software engineering," said Bolton, "how can we build the systems of the future that are likely to have billions of lines of code?"

The SEI-led team recognized that increased code size drove increased scale in many dimensions. These challenges strained existing software foundations. Therefore, achieving the Army's goal of information dominance depended on the availability of increasingly complex systems characterized by thousands of platforms, sensors, decision nodes, weapons, and users, all connected through heterogeneous wired and wireless networks. The SEI-led team called systems of such size, scale, and complexity "ultra-large-scale (ULS) systems."

According to the report's authors, the dominant characteristics of ULS systems would include decentralization, continuous evolution, widespread heterogeneity of constituent parts, and routine software and hardware failures. Articulation of these ideas spurred research initiatives both within and outside the SEI. Examples of these initiatives included the following:

- The SEI developed the architecture and infrastructure for the Army's Tactical Assault Light Operator Suit (TALOS), which supports the Army's goal of information dominance in the field by providing information superiority to the warfighter.
- Research conducted at the SEI in areas such as context-aware mobile computing, cyber-physical systems, socio-technical ecosystems, ubiquitous computing, self-adaptive computing, and tactical or "edge" computing grew directly out of insights in the report.
- Non-SEI collaborators on the report built on the report's insights in their own research, sparking advances in areas such as software ecosystems, modularity, and self-adaptive systems. The report also spawned graduate research, including a graduate specialization at Queens University in Canada in ULS systems, where students use the ULS report as a framework for their research.
- The report, published more than 10 years ago, has been widely cited in research literature and scholarly publications, including 144 citations between 2014 and September 2017.

What's more, the report accurately anticipated a future that has now arrived. As predicted in the report, systems are connected as never before, and the ramifications of this connectivity—decentralization; the need for resilience; massive interconnectivity of heterogeneous platforms; vast networks of wireless and wired devices; computational elements, automated devices, and humans co-existing as peers in cyber-physical, socio-technical ecosystems—continue to challenge the SEI and the communities it serves.

> **To learn more** about this and other topics discussed in the Year in Review, visit resources.sei.cmu.edu and search for "2017 SEI Year in Review Resources."

By creating exercises for events such as the Cyber X-Games, Cyber Flag, and Cyber Guard, the SEI provides challenging environments for DoD personnel to learn, compete, and apply their skills.

Researcher
AUSTIN WHISNANT

Bridging Science and Practice to Build Cybersecurity Knowledge and Skills

The Department of Defense (DoD) employs cutting-edge methods to defend against cyber threats, which continue to grow in scale and sophistication. In doing so, it works on three fronts. First, it collaborates with military and civilian experts in government, industry, and academic organizations to learn about—and adapt to—current and evolving cyber issues. Second, it enables its cyber defenders to share "attack and defend" best practices. Third, it integrates cyber operations into military operations.

To help the DoD meet these challenges, the U.S. Naval Postgraduate School (NPS) and Army Reserve Cyber Operations Group (ARCOG) sponsor the Cyber Endeavour conference. At this yearly event, thought leaders discuss issues that involve the Internet and national security in an environment that encourages thought-provoking discussion and interactive learning.

NPS and ARCOG selected Carnegie Mellon University to host Cyber Endeavour 2017 in part because it is home to the SEI. This year's event centered on the theme "Deterrence in and Through Cyberspace 2022: Threats, Concepts, and Solutions." The event attracted the nation's top minds in cyber defense, including policy officials, senior flag officers, interagency officials, cyber operators, and representatives from academic organizations. These thought leaders examined the problems of deterrence and discussed adversary strategies. Their discussions focused on threats, concepts, and solutions.

Cyber Endeavour was preceded by the Cyber X-Games, a five-day event in which attendees participated in large-scale cyberspace simulations and cyber-kinetic effects scenarios inspired by the conference theme. This year, 48 attendees working in five teams participated in the Cyber X-Games.

"Each team assumed the identity of a nation-state and participated in exercises simulating the defense and attack of networks," said the SEI's Austin Whisnant, who headed up the Cyber X-Games design. "Each nation-state team had an economy supported by a supervisory control and data acquisition (SCADA) system and a financial system, and was able to make purchases and use diplomacy. The teams also participated in a tactical simulation of a hostage rescue scenario."

The SEI hosts the Private Cyber Training Cloud (PCTC) technical infrastructure, the computing platform that served as the virtual environment for the Cyber X-Games and for many other cyber simulations. "This year, we incorporated Cyber Kinetic Effects Integration, a program we developed that enables the training of combined arms and cyber engagements in a virtual battlefield," said Whisnant. "We also used newly developed financial and SCADA simulations, a multi-team automated scoreboard, an intelligence repository, and the dark web." The Cyber X-Games form the basis for ARCOG's summer training and is one of the larger exercises the SEI develops and administers.

By creating exercises for events such as the Cyber X-Games, Cyber Flag, and Cyber Guard, the SEI provides challenging environments for DoD personnel to learn, compete, and apply their skills. Through collaborations like these, SEI researchers help bridge the gap between their research and development and the needs of the DoD.

Researcher
SATYA VENNETI

Making Biometric Data Extraction Mission Practical

Biometric traits such as heart rate, gaze, posture, and even facial microexpressions hold incredibly useful, but hidden, information. The ability to unobtrusively detect this information presents a number of potential applications that align with the mission of the Department of Defense:

- monitoring multiple subjects at security checkpoints
- finding live soldiers on the battlefield
- polygraphs and high-stakes meetings
- media analysis and exploitation
- machine emotional intelligence

This information is traditionally collected using monitors subjects must wear or in laboratories where subjects must remain completely still—constraints that aren't conducive to everyday settings in which subjects move around and lighting conditions vary.

Satya Venneti, of the SEI's Emerging Technology Center, is exploring passive biometrics, collecting information using non-invasive methods that require no physical contact with a subject and permit analysis in real time. Her work has produced a proof-of-concept prototype for extracting heart rates from subjects in natural settings using only a webcam.

"When the heart pumps blood through a subject's veins, the subject's face reddens slightly," explained Venneti. "We apply face landmarking to focus on the regions of the face where the changes are most pronounced—the forehead and cheeks. We then process the changes in each pixel across each frame using graphical processing units."

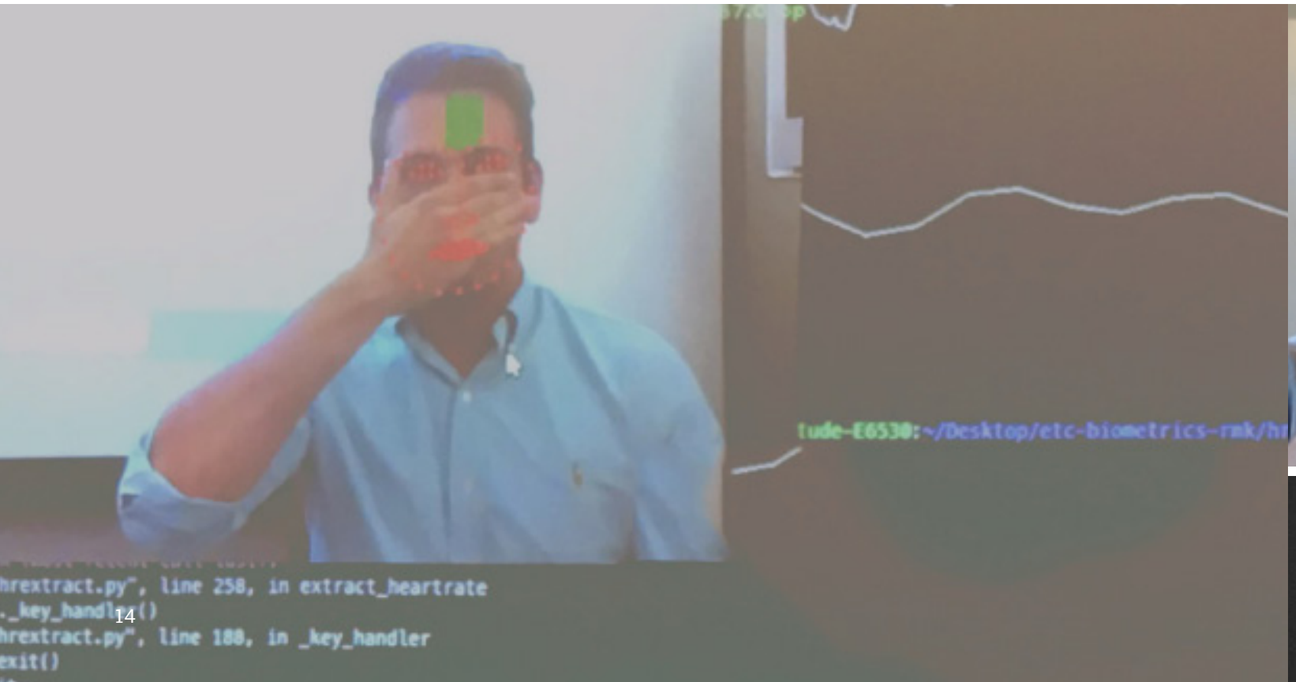
Graphical processing units (GPUs), with their massively parallel architectures, are the key to the real-time part of this project. Because they can handle a large number of parallel tasks at once, GPUs make it possible to determine heart rate in less than 15 seconds, the time it takes to get a sample for a reasonably accurate estimate regardless of what method is being used.

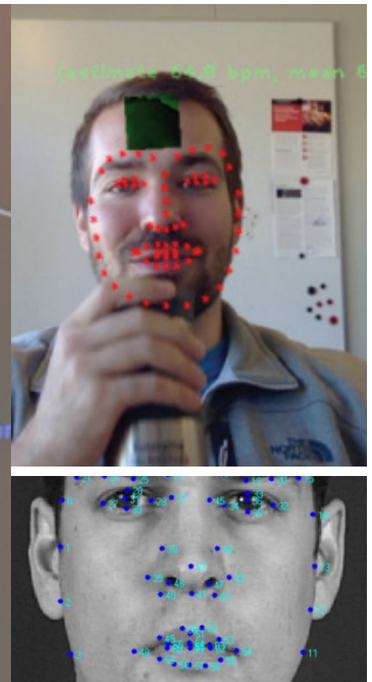
Venneti tested the prototype tool on a set of videos from the Imperial College of London. Because the videos captured subjects in natural settings along with their vital signs, they provided important ground truth for evaluating the accuracy of the SEI prototype. Venneti's prototype is accurate within two beats per minute.

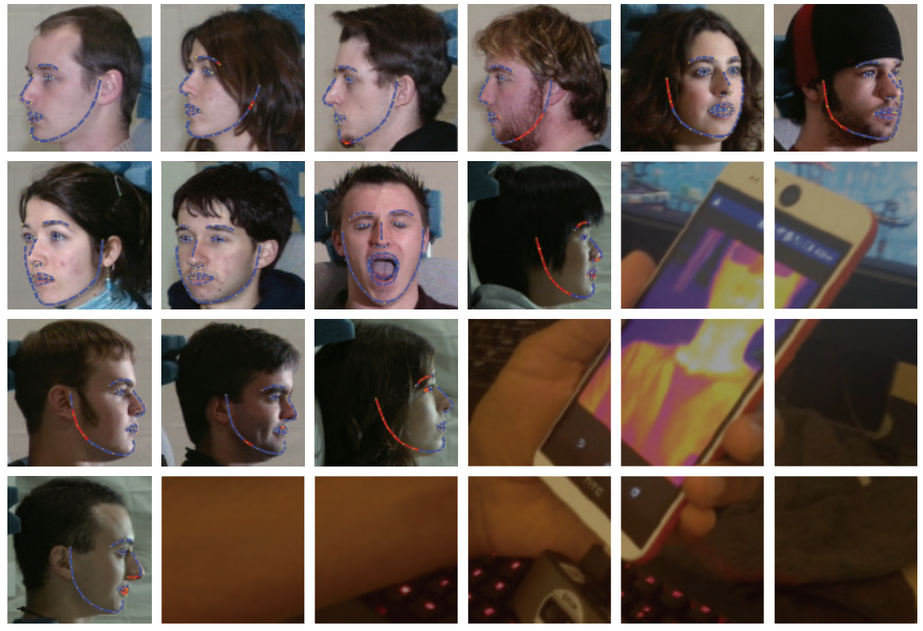
The tool was also used to successfully detect a spoofed face, a concern of many entities—especially government agencies—that are using biometrics for authentication.

Detecting heart rate is just the first step in what will likely become a portfolio of biometrics work for Venneti. "Looking to the future, we envision an approach that integrates various biometric features—heart rate, along with other traits (such as eye movement, voice frequency, and posture) that can reveal hidden information," said Venneti. "Our most recent work deals with microexpressions, nearly imperceptible movements in facial muscles that can reveal true emotions, even when someone is trying to hide how they really feel. We're already looking at ways to incorporate things like gaze and pose to detect where people focus or what they're going to do next." This integrated view can contribute to "machine emotional intelligence," enabling our technology to better interact with us and to better protect us.

> **To learn more** about this and other topics discussed in the Year in Review, visit resources.sei.cmu.edu and search for "2017 SEI Year in Review Resources."







Researcher
SCOTT MCMILLAN

Getting a Handle on Big Learning Platform Performance Measurement

"We're trying to measure as much as we can to determine what's important to measure."

—SCOTT MCMILLAN, SEI EMERGING TECHNOLOGY CENTER

Big learning—large-scale machine learning performed on big data—is becoming ever more complex. This type of machine learning uses large, complex models that must be managed, along with the data used to train them, and also uses increasingly complex parallel and distributed hardware and software platforms to speed up computation. When it comes to adopting the latest advances in big learning, organizations across sectors are faced with a tough problem: acheiving confidence in predictable results using their own platforms.

Predictable results are those that can be reproduced or extrapolated from the published results. "Few of the over 1,000 research papers published each year on machine learning include enough information to reproduce their results, and few give enough information to gain a more complete understanding of the performance characteristics," said the SEI's Scott McMillan. In those papers, researchers often devote most of their limited space to the accuracy of the trained models rather than documenting the configuration and various performance metrics of the computational frameworks (software) and hardware they used. Without this information, organizations can't be confident they can achieve the same results with their own platforms, which may differ from those used in experiments.

In 2017, McMillan and his team created the Performance Measurement Workbench to collect metrics about the performance of hardware components (such as CPU, memory, and disk) and software platforms processing machine learning algorithms. This work improves the reproducibility of reported results.

"With the Performance Measurement Workbench, we're trying to measure as much as we can to determine what's important to measure," said McMillan. For example, an organization might want to know whether a slight variation in memory, network bandwidth, or processor speed will affect performance for a certain machine learning algorithm. By collecting these metrics, the Performance Measurement Workbench can provide insight into which characteristics matter most for a particular computation.

The Performance Measurement Workbench runs within the cluster at the Carnegie Mellon University Parallel Data Lab. It collects metrics from a big learning platform of 42 compute nodes (each with a multi-core CPU and GPU accelerator) and a complex, tiered memory and storage system. Connected with a high-bandwidth, low-latency network, the cluster supports research in the development of parallel and distributed machine learning computing frameworks as well as the development and testing of large-scale metrics collection systems.

The Performance Measurement Workbench also provides a web-based portal on which researchers can configure and submit jobs, and analyze the metrics data collected. The portal offers operating system images with collection tools preconfigured and a persistent database to store the metrics, and visualization services to query and analyze the data. Users can also display the collected data live during computation or after an experiment has concluded. Behind the scenes, the Performance Measurement Workbench can also store the configuration information about the operating system, machine learning platform, and the algorithm as well as the commands used to invoke each component.

These features address two goals defined by McMillan and his team: ease of use and reproducibility. "With the Performance Measurement Workbench we have shown how consistent and complete metrics for big learning systems can be collected," said McMillan.


Researchers
JONATHAN CHU, PATRICK DWYER

Building Trust Between Humans and Autonomous Systems

"Trust is the key ingredient in human–robot interactions," said the SEI's Patrick Dwyer. With Jonathan Chu, Dwyer is addressing gaps in trusted human-system collaboration through innovative research and development. "Can people trust a robot to follow directions? Can they predict what it will do next? Will they need to constantly supervise it to make sure it correctly performs its tasks?" Dwyer explains.

Trust in autonomous systems (e.g., robots) is no small matter to the Department of Defense (DoD), where those systems are used to extend and complement human capability. These systems perform longer and without fatigue, reduce the data-processing workload on human analysts, operate in hazardous environments and at small scales, and react at speeds humans cannot match. However, unreliable, unpredictable robot behavior undermines the potential benefits of human-robot partnerships.

Giving Robots the Capability to Understand and Be Understood

The solutions that Chu and Dwyer created stem from this question: How can we team the robots and their operators to build trust and exploit autonomous behaviors? One answer Chu and Dwyer are exploring is the development of algorithms that allow robots to automatically explain their behaviors in human-understandable ways.

The team is also developing methods robots can use to provide cues to help humans understand and predict their actions—in part by finding ways to increase neglect tolerance, which is the length of time a human is willing to ignore a robot partner before actively monitoring it again. The less attention a human pays to its robotic teammate, the greater its trust. Chu and Dwyer gauge inattention by analyzing human gaze. "We looked at gaze tracking glasses as a way to measure the amount of time spent looking at the robot when operating," said Chu. "We hypothesize that as the robot behaves in progressively more predictable ways, humans will watch it less."

Further, the researchers are modeling trust-augmented specialized robot control interfaces. By adding information in the mission control interface, such as previous locations, points of interest, and navigational information, they are helping humans gain more trust and confidence in a robot's ability to complete a mission.

Assuring the Software that Makes Autonomy Possible

Finding ways to build trust in human–machine collaborations in mission contexts is important. Chu's team is exploring ways to make the software that comprises autonomous systems safer by working on enhancements to ROS-M. The public version of the open source Robot Operating System (ROS) provides libraries and tools for building robotic software systems. ROS-M, intended for military robots, builds on this framework by adding software and hardware simulation tools, cyber assurance checking, and validation and verification. It encourages code reuse and sharing, especially for components whose distribution is restricted for national security reasons.

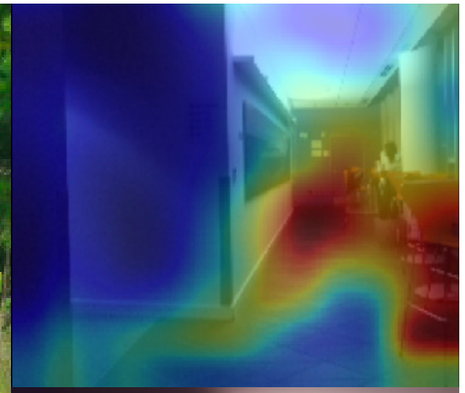
"Finding the right software components to build a robotic system can be challenging," said Chu. "Our work on ROS-M focuses on creating a registry of components that supports sophisticated, natural language-based queries. Developers will be able to search the registry to find components designed to work with specific hardware modules, run subsystems such as computer vision, comply with various standards, and meet security and integration requirements."

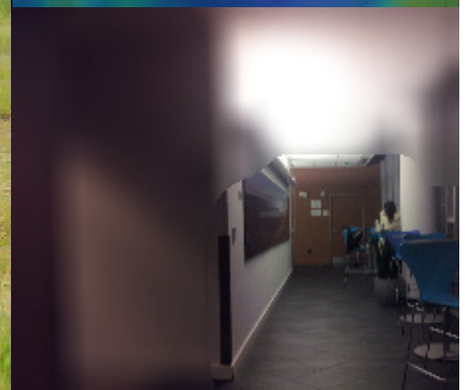
Chu plans to feed ROS-M improvements back into the public ROS release whenever possible. The defense robotics community will reap the benefits of faster innovation and improvements to the maturity of all robotic systems that use ROS. This will speed the development of reliable, trustworthy autonomous robots that can carry out a wide variety of missions, from cargo delivery to surveillance and reconnaissance.

The SEI's work on ROS-M is part of its support for the U. S. Army Tank Automotive Research, Development and Engineering Center (TARDEC), which researches and develops advanced technologies for unmanned ground systems.

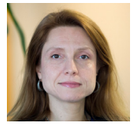
> **To learn more** about this and other topics discussed in the Year in Review, visit resources.sei.cmu.edu and search for "2017 SEI Year in Review Resources."


Photo: U.S. Army










Researchers
DAVID ZUBROW, ROBERT STODDARD, IPEK OZKAYA, WILLIAM NOVAK

SEI Research Combats Mounting Acquisition Costs

When the Department of Defense (DoD) wants to build a new weapon system or expand an existing system's capabilities, software increasingly plays a starring role. Software often demands the longest lead time of all system components, and it's expected to evolve over the entire life of the system. And though software makes many new capabilities possible, it is also increasing as a percentage of overall system costs. In 1997, software accounted for about 45 percent of a system's costs. In 2020, that number is projected to be 80 percent or more.

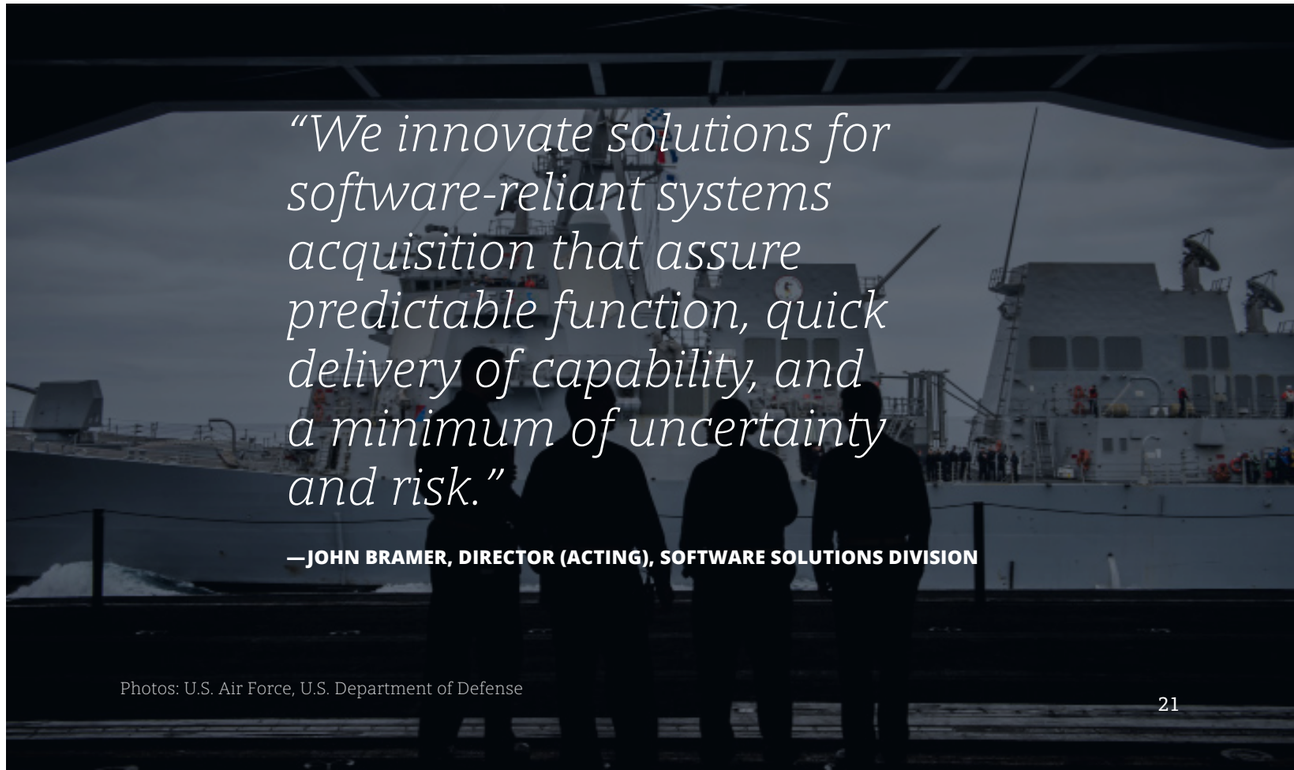
Because we are now in an era in which software costs can limit military capability, understanding and controlling these costs is critical. The SEI is attacking the problem in several ways, starting with analyses that provide a clearer picture of the current state of software development. The SEI's David Zubrow led the development of the *DoD Software Factbook*, an analysis of the most extensive collection of software engineering data owned and maintained by the DoD. "The *Factbook* is important because it translates raw data into information that is frequently sought after across the DoD, including how much a software system might cost and how long it might take to develop," Zubrow said. "It provides practical heuristics to estimate and improve program funding and plans going forward."

Several other lines of research at the SEI are getting at the root cause of rising software costs. "While important, it's not enough to know costs are going up or to accurately predict the increase," said Robert Stoddard, who is leading efforts at the SEI to apply causal modeling to large volumes of software development data. "To contain costs, we need to understand which factors drive costs and which factors we can control." By applying these new modeling and data-mining techniques, Stoddard looks to uncover relationships that will provide a basis for better acquisition policy, practice, and management.

Future anticipated rework, sometimes referred to as technical debt, has already been identified as a big contributor to rising software sustainment costs. The SEI is developing a clustering and ranking algorithm and prototype that can analyze and correlate data from multiple sources—including issue trackers, code repository histories, and static code analysis results—to identify the most significant design issues that contribute to technical debt. "Enabling the identification of design issues and quantifying their impact on sustainment and modernization efforts will provide data the DoD needs to control lifecycle costs, mitigate technical risk, and reduce cycle times, all goals of the Better Buying Power initiative," said the SEI's Ipek Ozkaya.

Another way of combating rising software acquisition costs is to improve efficiency by making sure contractors cooperate, which is becoming harder to do as government programs move away from the use of a lead systems integrator. Misaligned incentives among contractors, or with the program management office, can cause wasted effort, lost time, and poor results. The SEI's William Novak is leading a research effort that uses game theory to frame these situations, then applies agent-based modeling to quantify and evaluate them. "Different types of incentives—financial, strategic, and social—affect contractors to different degrees," said Novak, "and the combined impact of multiple incentives can be more effective across a range of contractors in changing their behavior." This research allows the simulation of candidate incentive mechanisms, in the context of an acquisition program model, to see which combinations of contractor incentives can produce the best acquisition outcomes. This approach, which is being piloted, shows promise for solving some of the incentive problems that can plague acquisition performance.

> **To learn more** about this and other topics discussed in the Year in Review, visit resources.sei.cmu.edu and search for "2017 SEI Year in Review Resources."



"We innovate solutions for software-reliant systems acquisition that assure predictable function, quick delivery of capability, and a minimum of uncertainty and risk."

—JOHN BRAMER, DIRECTOR (ACTING), SOFTWARE SOLUTIONS DIVISION

Photos: U.S. Air Force, U.S. Department of Defense

Transitioning Research Results through Open Source Tools

Moving research results into practice in the Department of Defense (DoD), government, and defense-related industry is central to the SEI's purpose. One transition path we use is to develop and deploy tools that fortify the nation's technological edge over adversaries and strengthen the development practices of DoD software contractors. In FY17, the SEI released more than two dozen new and updated tools for public, DoD, or federal agency use.

The SEI's publicly available, open source tools released recently include

Pharos
This static analysis framework facilitates the automated analysis of binary programs, with a focus on malicious code analysis. Pharos builds upon the ROSE compiler infrastructure developed by Lawrence Livermore National Laboratory.

SeaHorn
The SEI's innovation in this software model checking framework is to use Horn clauses to represent verification conditions. SeaHorn provides developers a powerful verification tool and researchers an extensible platform that simplifies the development and integration of new verification techniques.

KD-Cloudlet
This software tool implements tactical cloudlets, which are discoverable, generic, virtual-machine-based, stateless servers located in single-hop proximity of mobile devices.

Vulnerability Analysis Tools
The tools the SEI offers for vulnerability analysis incude BFF and Dranzer. The CERT® Basis Fuzzing Framework (BFF) is a software testing tool that finds defects in applications that run on Linux, Mac OS X, and Windows. Dranzer enables users to examine effective techniques for fuzz testing ActiveX controls.

DART algorithms and tools
In distributed adaptive real-time (DART) systems, such as ensembles of unmanned air systems, physically separated nodes communicate and coordinate to achieve their goals and self-adapt to their environment to improve the likelihood of success. These algorithms and tools support DART system requirements for high-assurance and certification of safe, effective operation

OSATE
The Open Source AADL Tool Environment (OSATE) supports Version 2 of the Architecture Analysis and Design Language (AADL) industry standard for representing the architecture of large-scale, software-intensive, embedded systems and systems of systems, such as aircraft, spacecraft, autonomous systems, and medical devices.

CERT Linux Forensics Tools Repository
These tools and toolsets improve the effectiveness of cyber forensics acquisition and analysis practitioners.

CERT SiLK
The System for Internet-Level Knowledge (SiLK) offers a set of tools for network traffic analysis.

Enabling Evidence-Based Modernization
Stakeholders can use this decision-support tool to identify key decisions that influence the quality of a chosen solution for business system modernization.

BigGrep
With this tool, users can index and search a large body of binary files. BigGrep uses a probabilistic n-gram-based approach to balance index size and search speed.

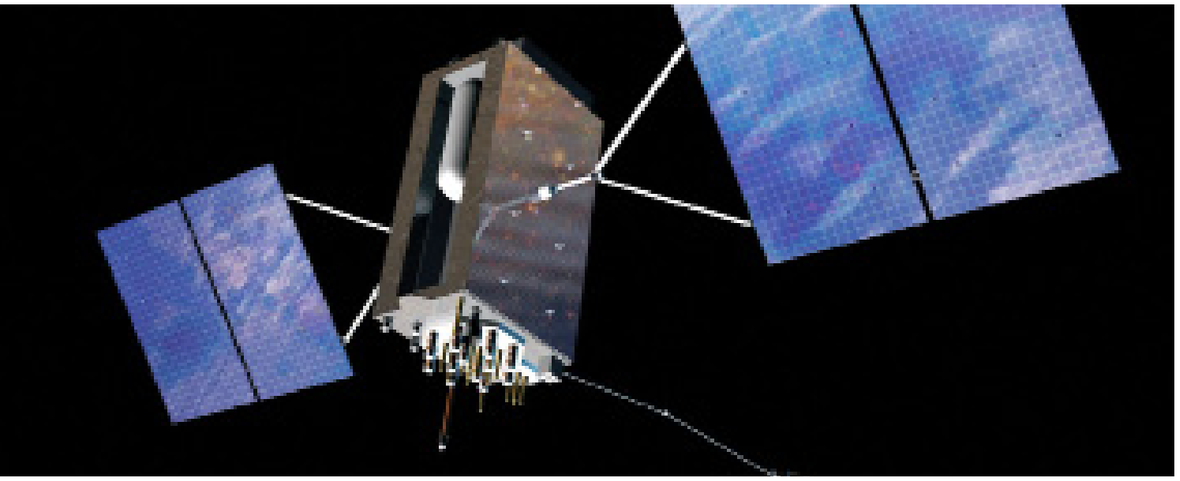
Look for all SEI tools on our website at http://www.sei.cmu.edu/tools/.

"We focus on how the DoD and other government organizations can make the most of innovative, recently possible technologies, through research and tool development that will enable our sponsor and other organizations to apply these advances to mission challenges."

—MATTHEW GASTON, DIRECTOR, EMERGING TECHNOLOGY CENTER

Researcher
JOHN ROBERT

Ready, Capable Teams Enable the SEI's Rapid Response



For more than three decades, the SEI has been building a reputation for technical expertise and experience that has made its staff "the people you call" when you have a big software problem in need of a timely solution. Drawing on its research program achievements and core competencies in software engineering, cybersecurity, and acquisition, the SEI delivers rapid response to Department of Defense (DoD) programs needing help with time-sensitive weapon system projects and cyber incident resolution.

SEI researchers from across the institute explore numerous areas of concern to the DoD, including acquisition processes, system modernization, and assessments of the mission readiness of cyber operators at scale. "Research such as this puts our experts in frequent contact with organizations across the DoD," said the SEI's John Robert. "In the process, we learn a lot about our sponsors' programs and systems—and the real-world challenges they confront every day."

Informed by both research and real-world experience, our experts bring to the table a well-rounded, integrated set of capabilities and skills, and they tackle many diverse challenges confronting the DoD and government—everything from applying Agile development principles in government settings to institutionalizing cybersecurity practices across a program or organization.

"Our knowledge of DoD environments and our ongoing research program position us to rapidly respond when called on by our sponsors," said Robert. Recent examples from FY17 include support for a key satellite system, in which SEI staff applied the knowledge they gained through research on DevOps and acquisition incentives; support for the development of a new Navy program, which leveraged SEI research on software analysis and automating software standards compliance; and a modernized Air Force missile system, in which the SEI's research on Agile development, software acquisition strategy, and modernization played key roles.

Photo: U.S. Air Force

Researcher
RITA CREEL

Supporting Security and Resiliency for Air Force Missions

The U.S. Air Force has undertaken a comprehensive effort to build cyber resiliency into new weapon systems and mitigate critical vulnerabilities in systems currently in the field. The SEI is employing its expertise at the nexus of software engineering and cybersecurity to support this work, which is managed by the Air Force Cyber Resiliency Office for Weapon Systems (CROWS). CROWS is executing work across seven lines of action: analyzing cyber impacts on the mission; integrating security and resiliency engineering into systems engineering; developing a cyber-aware acquisition workforce; applying open systems architectures to enhance adaptability and resiliency; ensuring a common security environment; mitigating vulnerabilities in legacy systems; and applying cyber intelligence to acquisition and engineering.

The SEI joined the effort in 2015, partnering with other federally funded research and development centers and university-affiliated research centers on the Air Force Security Engineering Team (AFSET). The SEI's software–cyber perspective is an essential complement to the skills of other AFSET members. Recently, the AFSET delivered an assessment of science and technology challenges for cyber resiliency, with work in progress on a set of key system resiliency activities for Air Force programs. In 2016, the SEI joined with MITRE to pilot a RAND-developed approach that prioritizes systems for detailed cyber vulnerability analysis based on projected impacts on mission thread execution. Following the pilot, SEI team members recommended improvements to the approach and are exploring the use of software architecture models and measures to improve the resultant prioritization.

"We are committed to helping the Air Force achieve its goal to acquire, operate, and sustain cyber-resilient systems for assured mission success," said the SEI's Rita Creel. "Given the critical risks associated with software and the growing reliance on software for mission capability, the SEI's blend of expertise is in high demand. The effort to build and sustain secure software that supports cyber resiliency begins early in acquisition, long before a line of code is conceived, and continues throughout the lifecycle."

In addition to Creel, the SEI's Chris Alberts, Carmelita Caudle, Harold Ennulat, Mark Kasunic, John Klein, Chris Miller, Mary Popeck, Alexis Presti-Simpson, and Carol Woody contributed to this work.

> **For more information** on the SEI's work in DoD acquisition support, visit sei.cmu.edu/acquisition.

Photo: U.S. navy

"... DVDP was a great exercise in applying and modernizing coordinated vulnerability disclosure lessons learned during the past few decades."

—ART MANION, SEI CERT DIVISION

Photo: U.S. Department of Energy

Researcher
ART MANION

Reporting DoD Network Vulnerabilities Just Got Easier

Almost 30 years ago, the SEI's CERT Coordination Center established a program that enabled security researchers in the field to report vulnerabilities they found in an organization's software or system. But this capability did not always include vulnerabilities found on Department of Defense (DoD) sites. In 2017, the SEI helped expand vulnerability reporting to the DoD by establishing the DoD Vulnerability Disclosure Program (DVDP).

The DoD began evolving toward its modernized vulnerability disclosure policy in 2016. Realizing the value of contributions that security researchers make to the security of the Internet, the DoD forged a relationship to encourage their testing and reporting for DoD sites. First, it introduced two successful bug bounty programs—"Hack the Pentagon" and "Hack the Army"—that rewarded registered participants with cash payouts for reporting verifiable vulnerabilities. These programs were intentionally limited in length and scope.

The DoD then engaged the SEI to develop a longer running program. In 2016, it tasked the institute with developing a policy to provide clear guidance for security researchers on disclosing vulnerabilities found in any DoD public-facing website or system. Ash Carter, then Secretary of Defense, was a strong proponent of this "see something, say something" policy, and he expressed satisfaction with its success in bolstering the department's—and the nation's—security.

The DoD soon realized the need for its own vulnerability disclosure program. In FY17 the SEI, working with the DoD Cyber Crime Center (DC3), transitioned the knowledge gained from its experience and vulnerability analysis research to help establish the DVDP. The SEI helped design the process and handled inbound reports from researchers, validating vulnerabilities, passing them to the DC3 for mitigation, and later validating the applied fixes.

"Currently, we work in process engineering, policy, and reach back, rather than day-to-day operations," said Art Manion, vulnerability analysis technical manager in the SEI's CERT Division. "Our mission is to transition the process."

Manion sees the need for many more organizations to adopt the process. The *CERT Guide to Coordinated Vulnerability Disclosure*, published in 2017, provides a comprehensive guide for establishing a successful CVD program. Written for vulnerability analysts, security researchers, developers, and deployers, it serves both technical staff and their management.

As the guide makes clear, CVD is a socio-technical challenge, requiring collaboration among vendors, researchers, and other stakeholders. "While pinpointing the vulnerability and fixing it is technical," said Manion, "the rest is process and policy and trying to get things done effectively without causing people undue stress and work."

"Helping to design and operate the DVDP was a great exercise in applying and modernizing coordinated vulnerability disclosure lessons learned during the past few decades," added Manion. "The DVDP is a permanent and long-term program—there's no time boundary on it, and it applies to all DoD websites; that's a lasting way for the DoD to take in external vulnerability reports."

> **To learn more** about this and other topics discussed in the Year in Review, visit resources.sei.cmu.edu and search for "2017 SEI Year in Review Resources."

Researcher
DIONISIO DE NIZ

Assuring Autonomous Systems That Operate in Mission Environments

Distributed, adaptive real-time systems consist of several agents that communicate and coordinate to achieve their goals; for instance, a fleet of unmanned aerial vehicles operating in a shared airspace. They self-adapt to their environment—in the air, on the ground, and under water—to improve their likelihood of success. This smart adaptation promises to help the Department of Defense (DoD) achieve its mission in contested environments and is a key component of the DoD Third Offset Strategy.

Achieving assurance in software with autonomous features is challenging because uncertainty exists in the physical environment, and autonomous capability leads to unpredictable behavior. The Defense Advanced Research Projects Agency (DARPA) recently launched the Assured Autonomy Program to seek solutions to these problems, recognizing that today's assurance methods do not adequately address machine-learning capabilities. As SEI principal researcher Dionisio de Niz explained, "Software with machine learning is hard to certify. This software learns, but you don't know exactly what it will learn."

Machine learning enables so many behavior variations that these components cannot be verified before deployment. Instead, they are coupled with runtime assurance, which involves adding a "watchdog," called an *enforcer*, to monitor the behavior of the system and prevent behaviors that could lead to unsafe results. The solution developed by de Niz and team encodes runtime policies into enforcers and a tool to verify the correctness of these enforcers' implementation against those policies. It also uses an algorithm to check consistency among multiple enforcers working on the same component and to verify that they collectively implement a global safety policy. This method of formal algorithm verification ensures that autonomous systems operate within safe bounds.

De Niz describes the algorithms as "simple enough to be verified at the source-code level." Because they control the enforcers, which can control the system if it exhibits unsafe behavior, "this arrangement allows the system to be verified for safety," de Niz noted. The SEI is advancing this approach with a method called continuous runtime assurance. As the system is modified to add new features, new enforcers are added, and their consistency with previous enforcers is verified. This is important because autonomous systems have multiple safety-critical requirements that may produce conflicting commands. These systems have functional and timing requirements; an event must happen, but if it happens at the wrong time, the mission could fail.

The SEI team tested its solution at the Air Force Research Laboratory (AFRL) Summer of Innovation, an event that brought academia and industry together to advance research on verifying the safeness of software and reliability of autonomous code. Using AFRL's UxAS, a service-oriented software system for operating unmanned vehicles, the SEI simulated a mission with distributed unmanned aerial vehicles (UAVs). A logical enforcer modified a UAV's path depending on whether the UAV detected an enemy in the area, and a temporal enforcer triggered the UAV to circle if it needed more time to verify whether the next action was safe. Together, these simple logical and temporal enforcers achieved a verifiably safe system.

> **To learn more** about this and other topics discussed in the Year in Review, visit resources.sei.cmu.edu and search for "2017 SEI Year in Review Resources."

"Software with machine learning is hard to certify. This software learns, but you don't know exactly what it will learn."

—DIONISIO DE NIZ, SEI SOFTWARE SOLUTIONS DIVISION

Photo: U.S. Army



Researchers
JOSH HAMMERSTEIN, JEFFREY MATTSON, GRACE LEWIS

Pushing R&D to the Front Lines

The Department of Defense (DoD) seeks to increase mission effectiveness in tactical settings by, in part, providing warfighters greater mobility. One way to do this is to untether warfighters' devices from set locations and ensure secure access to the information and services the warfighters need to fulfill their mission. The challenge of these tactical settings, which are found in all five warfighting domains (land, sea, air, space, and cyberspace), is a computing environment often characterized by limited power and network resources.

To help meet this challenge, the SEI has invested DoD funding over several years in applied research and development for computing, communications, and analytics in tactical settings. In FY17, this work involved integrating cyber effects with tactical operations, providing Internet of things (IoT) authentication in constrained environments and releasing a new version of a software tool to aid computing in tactical environments.

Using Augmented Reality to Visualize Cyber-Warfare Opportunities

Frontline warfighters have difficulty considering cyber effects during tactical missions because of the abstract nature of cyberspace. A cyber effect can be either an offensive or defensive action in cyberspace intended to produce a desired outcome on a system or a device. In new research, the SEI's Josh Hammerstein and Jeffrey Mattson led a team creating cyber affordances to help warfighters visualize cyber-warfare opportunities in their natural surroundings. In a tactical setting, an affordance can show a relationship between an environment and a warfighter. The SEI approach uses augmented reality to display virtual content in the form of 3D graphics aligned and overlaid on the real world.

"Warfighters can expand their arsenal through greater awareness of specific lethal and non-lethal cyber tactics," said Hammerstein. "For example, a warfighter on a reconnaissance mission who enters a potentially hostile or dangerous space, such as a storefront in enemy territory, might be able to gain access to an open wireless access point in the area or exploit vulnerabilities in the building's alarm-communication system."

Computing with KD-Cloudlet in Tactical Settings

The sensors and devices that cyber affordances rely on require computing power not always available in tactical settings. Building on earlier SEI work to move cloud computing into tactical settings, the SEI's Grace Lewis released a new version of KD-Cloudlet, an open source software tool for implementing tactical cloudlets. Lewis's work employs the cloudlet concept created by Mahadev Satyanarayanan of Carnegie Mellon University's School of Computer Science. A cloudlet is a discoverable, generic, stateless server located in single-hop proximity to mobile devices. Hosted in the field on vehicles or other platforms, tactical cloudlets provide forward data-staging for a mission, infrastructure to offload computation from mobile devices, and other benefits. KD-Cloudlet is available in the CMU SEI open-source code repository on GitHub.

Establishing Trust in Disconnected Environments

Lewis is also involved in a project that addresses authentication and authorization for IoT devices in edge environments. Because connecting mobile devices and network-enabled sensors expands the attack surface in resource-constrained and adversarial environments, existing IoT security approaches are insufficient. To address this concern, Lewis led a cross-functional team in analyzing, extending, and influencing a proposal by the Internet Engineering Task Force (IETF) Authentication and Authentication for Constrained Environments (ACE) Working Group. The proposal now addresses high-priority threats in tactical environments, such as node impersonation and capture, and it considers operations in disconnected, intermittent, limited environments.

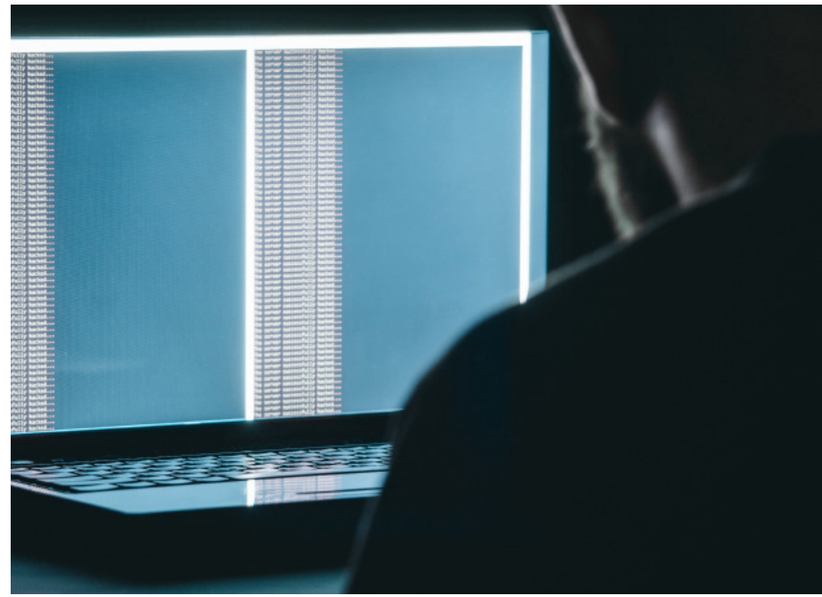
Combining its competencies in software engineering and cybersecurity, the SEI is pushing its applied research and development to meet the needs of warfighters in tactical settings for computing power and security.

> **To learn more** about this and other topics discussed in the Year in Review, visit resources.sei.cmu.edu and search for "2017 SEI Year in Review Resources."

Photos: U.S. Army and U.S. Department of Defense

Researcher
ANDREW MELLINGER

Enabling Elusive Systems: Adaptive Cyber Defense for Networks



Common sense dictates that a moving target is harder to hit than a stationary target, yet traditional network defense systems have been built around the fortress model. This is why in recent years the government has invested substantially in the rapidly growing field of moving target and adaptive cyber defense. This field has spawned many new technologies, but researchers need a centralized reference platform on which new technologies can be vetted and evaluated against a common standard. To meet this need, researchers at the SEI's Emerging Technology Center (ETC) are leading a multi-year project to develop a secure, easy-to-use, consistent development and deployment path to organize dynamic defenses.

Dynamic network defenses are adaptations to a system that create unpredictable conditions for cyber attackers. "When most people think about defense, whether it be a network or a physical entity, they think about a static set of defenses," said the ETC's Andrew Mellinger. "But static defenses allow attackers the opportunity to understand and get around them."

A dynamic defense, explained Mellinger, can turn any technical attribute (for instance, schema, format, or protocol) into a moving target. Two well-known dynamic defenses are Internet protocol hopping, which strengthens networks against distributed denial-of-service attacks, and address space layout randomization, which protects against buffer overflow attacks.

To facilitate development in this area, researchers from the ETC have been working to create a reference implementation for a dynamic network defense platform—a standard by which future implementations and customizations can be evaluated.

Mellinger's team is collaborating with Marco Carvalho, a professor at the Florida Institute of Technology (FIT). He is also working with David Garlan and Bradley Schmerl, experts in self-adaptive systems who work for the Institute for Software Research (ISR) at Carnegie Mellon University's School of Computer Science (SCS). Collectively, these three researchers have published dozens of papers in the past decade on self-adaptive systems. More recently, they have focused on applying their research to security.

The team's approach blends self-adaptive systems with multi-agent systems. Self-adaptive systems can evaluate and modify their own behavior to improve efficiency. They feature a central-reasoning component that can be used to ensure properties such as resiliency, healing, optimizations, configuration, and protection. Multi-agent systems, a loosely coupled network of software agents that interact to solve problems, are resilient and partition tolerant. And because they are decentralized, they provide additional redundancy that minimizes the risks of single points of failure.

"Our approach also includes strong human-in-the-loop support," said Mellinger. "Our goal is to ensure that system administrators defending the network will have a role in decision making and that the system's defenses will be transparent to defenders." This human-in-the-loop support extends to an approval component for changes proposed by the autonomic system.

Dynamic defenses offer many promising solutions for protecting vulnerable systems against attack. With substantial investment in the development of dynamic defense resources, developers, researchers, and system administrators need a common environment in which solutions can be compared and tested for compatibility.

"Our platform will offer measurable improvements in security posture for real networks and will also allow researchers to evaluate new technologies in a standard environment," said Mellinger. "It will also allow researchers to classify moving target strategies while facilitating experimentation, prototyping, and collaboration."

> **To learn more** about this and other topics discussed in the Year in Review, visit resources.sei.cmu.edu and search for "2017 SEI Year in Review Resources."

Researcher
CHRIS MAY

Anywhere, Anytime Training for Cyber Operators

Because cyberspace is such a dynamic environment, cyber operators in the Department of Defense (DoD) must continuously sharpen their skills and develop new knowledge and experience to ensure mission readiness. In other words, they must train as they fight. To help deliver training that meets the DoD's specialized needs, SEI researchers developed the Simulation, Training, and Exercise Platform (STEP). This web-based learning platform provides convenient, hands-on, extensible, and scenario-based environments that deliver realistic and cost-effective training.

This training helps cyber operators conduct both offensive and defensive cyber missions to protect U.S. cyber systems from unauthorized access and attack. Under direction from U.S. Cyber Command and its service component commands, cyber operators are DoD team members in the Cyber Mission Force who combat our nation's adversaries to ensure U.S. freedom of maneuver in the cyberspace domain.

One of the many ways the DoD uses STEP is to provide cyber operators asynchronous classroom instruction and synchronous exercises to create a dynamic and customizable training experience that is available anywhere, anytime. In this way, STEP meets cyber operators' needs for access to high-fidelity training.

"STEP delivers realistic scenarios that replicate operational missions and the challenging and stressful situations cyber operators confront in the real world," said the SEI's Chris May, technical director of the Cyber Workforce Development Team.

Currently, more than a dozen STEP instances are running at various classification levels across numerous DoD military installations. This persistent training environment plays host to two major training exercises: Cyber Flag and Cyber Guard. "For these exercises, the SEI creates hundreds of virtualized enclave networks and makes them come to life with game-changing simulators," said May. These SEI software prototypes replicate advanced user activities, wireless, novel malware, industrial control systems, and even the entire Internet—all within a single virtual machine.

Photo: U.S. Army

To help the DoD measure the effectiveness and performance of individual cyber operators and teams, STEP includes advanced, performance-based assessment technology. And because mission readiness must be demonstrated within realistic conditions, not just evaluated using traditional exams, STEP also includes cyber-kinetic effects integration for cross-domain training. To complement these features, the SEI equips STEP with a powerful dispatcher control framework that enables completely hidden modification and evaluation of massive cyber exercises as well as single-operator assessments.

Though designed as a training platform, some organizations extend STEP to other purposes. For instance, STEP allows organizations to simulate or test new platforms and software with confidence because it provides needed data and insights without compromising the value of interacting with live systems.

"We think STEP provides the DoD an effective tool for training its cyber operators in cutting-edge cyber defense techniques, helping them to outmatch our adversaries," said May. "And it gives the DoD a good way to measure the preparedness of its cyber warrior teams."

> **To learn more about STEP,**
> visit https://stepfwd.cert.org



Researchers
EDWIN MORRIS, LORI FLYNN, SARAH VINSKI

A Fighting Chance: Arming the Analyst in the Age of Big Data

Security and defense often come down to a numbers game. The Department of Defense (DoD) needs more trained analysts, and the analysts it fields must process an exploding volume of sensor and intelligence data. The SEI is working on several fronts to help develop qualified analysts, to help the DoD get more out of every analyst it fields, and to help DoD analysts operate at the pace of the adversary.

Tactical Analytics

An SEI team led by Edwin Morris is developing an edge analytics pipeline for streaming situational awareness. The team first created a platform for building and testing data analytics for streaming textual data. It then tested this platform by analyzing social media and other communications in large public-safety settings, such as multi-day music festivals and sporting events.

Building on this work, Morris's team began developing algorithms for extracting patterns of life (or "scripts") from video and streaming data. A script represents a stereotypical sequence of events and interactions in a particular context. Scripts help analysts relate emerging situations, captured in large volumes of streaming data, to what is already known (such as the typical sequence of events observed when ISIS takes over a village). "Our long-term goal," said Morris, "is to build the pipeline to recognize events in streaming data, determine the credibility of those events, and extract the scripts for interpolation and extrapolation by analysts."

Prioritizing Alerts from Static Analysis

The SEI's Lori Flynn leads a project that uses classification models to help analysts and coders prioritize which static analysis alerts to address. This is a tough problem for analysts who must validate alerts generated by one or more static analysis tools used to identify many potential code flaws. The effort required to manually audit all alerts and repair all confirmed code flaws is often too much for one analyst (or even a group of analysts) to perform, and doing so would exceed a project's budget and schedule.

Flynn's approach to this problem draws on past work in areas such as code contextual information, alert type selection, data fusion, machine learning, and mathematical methods for sorting true and false alerts. It also builds on work in the areas of dynamic detection, graph theory, and model checking. The goal is to produce a statistical classifier that will enable software analysts and coders to prioritize which alerts to address by automatically

- calculating the confidence that an alert is true or false
- partitioning alerts into three categories: expected true positive, expected false positive, and indeterminate
- ordering the alerts in the indeterminate category using a confidence metric

To test its approach, Flynn's team is collaborating with three DoD organizations that must address static analysis alerts generated for their codebases, which exceed 100 million significant lines of code. "We expect the organizations to collectively generate approximately 662,000 alerts," said Flynn. "Our goal is to classify 90 percent of flagged anomalies as true and false positives with 95 percent accuracy."

Education and Training

In 2016, the U.S. Army Cyber Command (ARCYBER) tasked the SEI's Cyber Workforce Development (CWD) team with creating training courses for Defense Information Systems Agency's Big Data Platform (BDP). The BDP consists of multiple services and tools, including popular open source big data and cloud computing solutions, such as Hadoop and Spark. It also includes custom services and applications. Hands-on interaction with the BDP interface is required to properly train ARCYBER computer protection teams and operations research systems analysts.

The CWD hosts and maintains its own multi-node training instance of the BDP. The services on the BDP are closely integrated and must be monitored to ensure that the BDP is running properly. The SEI's training instance of the BDP and the course material are updated to align with the latest version of the BDP.

"The BDP gives the Army and other branches of the military resources for leveraging big data for cybersecurity applications, but the Army has a gap in personnel trained in big data analytics and data science," said the SEI's Sarah Vinksi. "Our modules and training instance of the BDP are being used to address this issue."

The first course developed by the SEI is an introduction to the BDP. It consists of video lessons, hands-on labs that use the training instance of the BDP, and an analyst workstation students can use for each lesson. A second course focused on data science, R. Shiny applications, and Spark analytics is in development.

By developing these tools, methods, and educational resources, the SEI is doing its part to help the DoD get the most out of its analyst resources by helping them keep up with an ever-changing environment and growing volumes of data.

Photo: U.S. Army

“There has never been a greater need to address the persistent and growing cybersecurity risks that threaten the nation’s defense, homeland security, and intelligence communities.”

—PAUL D. NIELSEN, SEI DIRECTOR AND CEO

Building the Cyber Capacity of International Partners

Strategic Goal 5 of the 2015 Department of Defense (DoD) Cyber Strategy concerns building capacity for partners by helping to improve the cyber capabilities of allies in regions important to U.S. military and diplomatic strategy. To accept U.S. military aid, allies must ensure their networks and operations are sufficiently secure to accept the new platforms the U.S. State Department provides through foreign military sales. The SEI’s CERT Division is working with its DoD sponsor to ensure these nations have sufficient cyber capabilities to accept these new systems.

In addition to assessing capabilities and providing training, one way the SEI supports U.S. allies is by helping them set up computer security incident response teams (CSIRTs). A CSIRT is a service organization responsible for receiving, reviewing, and responding to computer security incident reports and activity. A CSIRT with national responsibility (or national CSIRT) is a CSIRT that has been designated by a country or economy to have specific responsibilities in cyber protection for the country or economy.

Since the 1980s, the SEI has been at the forefront of efforts to create and support CSIRTs by delivering training, publishing extensive guidance, and providing direct assistance. CERT founded the Forum of Incident Response and Security Teams (FIRST) in 1990 and administered FIRST until 1999, when FIRST evolved to a non-profit organization led by an international community of members. FIRST holds an annual Conference on Computer Security Incident Handling at which the SEI continues to play an active role. Each year at the FIRST Conference, the SEI holds a national CSIRT meeting. The 2017 meeting was held in San Juan, Puerto Rico, and was attended by 38 countries.

Another example of the work the SEI undertakes on behalf of our international partners is a recently concluded engagement to advance and develop cybersecurity capacity at the Côte d’Ivoire national CSIRT (CI-CERT). The engagement, which began in January 2015, was organized by the State Department as part of a larger effort to develop cybersecurity capacity in Sub-Saharan Africa.

The SEI sent a team to Abidjan, Côte d’Ivoire to conduct a five-day advanced incident-handling workshop. The purpose of the workshop was to expose CI-CERT analysts to needed skills in the areas of artifact analysis, log analysis, and vulnerability handling, all of which are needed to address advanced incidents. SEI personnel lectured on a variety of incident-handling topics and conducted practical exercises that provided participants an opportunity to practice the skills they learned in the lectures.

The workshop followed a two-year period in which the SEI and the State Department worked to integrate CI-CERT with the international CSIRT community by becoming an official member of FIRST. CI-CERT’s application was approved by the FIRST Board in September 2016.

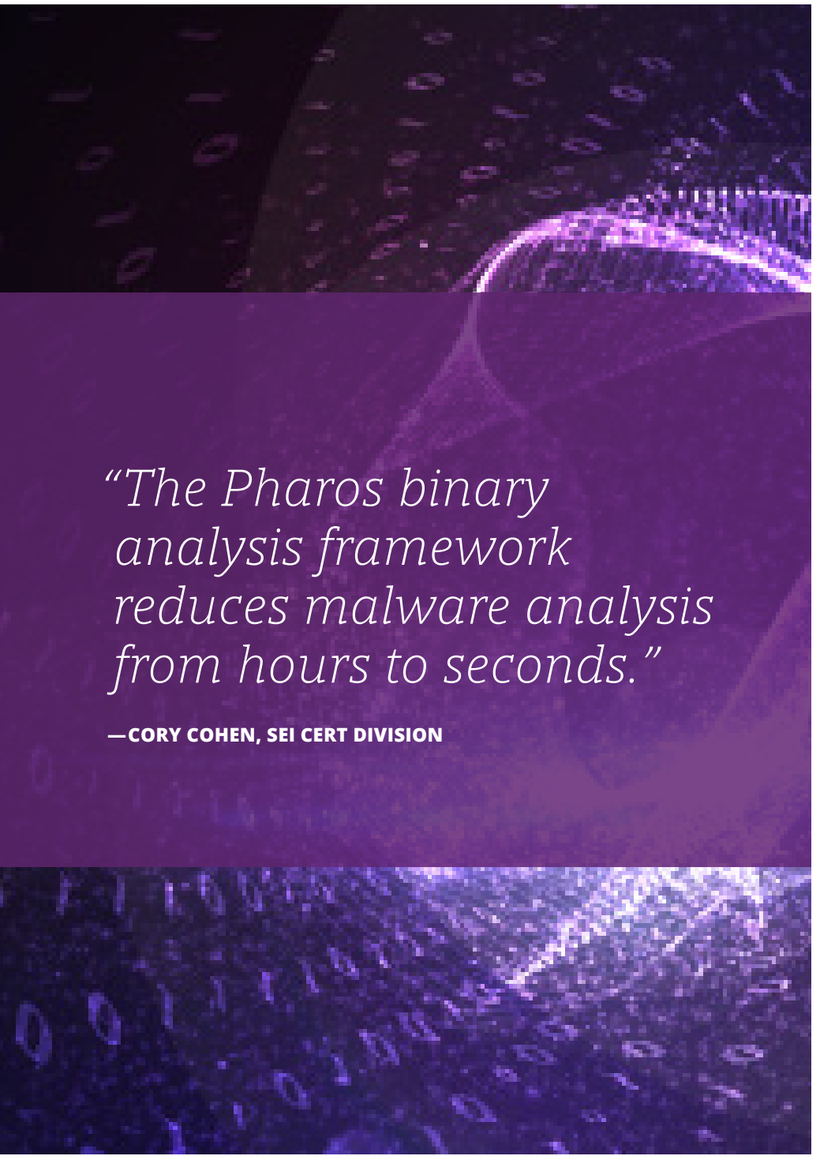
The SEI continues to advise and train personnel from other countries, including Ghana, Senegal, Botswana, and Kenya in Africa; Vietnam, Indonesia, Myanmar, and the Philippines in East Asia and the Pacific; and countries in Europe. Through these engagements, the SEI helps its international partners understand how to stand up needed cybersecurity capabilities and collaborate with the broader community on a regional and international basis.

> **To learn more** about this and other topics discussed in the Year in Review, visit resources.sei.cmu.edu and search for “2017 SEI Year in Review Resources.”



Researchers
CORY COHEN, ED STONER, WILL KLIEBER

Automated Code Analysis and Transformation



"The Pharos binary analysis framework reduces malware analysis from hours to seconds."

—CORY COHEN, SEI CERT DIVISION

At the Department of Defense (DoD), conducting malware analysis, detecting and patching software flaws, and discovering vulnerabilities have been manual, expensive processes that are both time and labor intensive. The same goes for ensuring software conforms to secure coding principles, detecting and fixing coding errors, and keeping pace with adversaries. What's more, increasing software complexity makes it even harder for DoD analysts to perform these essential tasks. To address these challenges, the SEI has undertaken several lines of research and development.

Automating Malware Analysis with Pharos

SEI researchers are using advanced program analysis to automate how analysts understand malware behaviors and find and fix coding errors that lead to software vulnerabilities. Automating malware analysis will reduce the cost of this work. The SEI's Pharos binary analysis framework allows deep, static malware analysis tools to be developed quickly and easily. "Pharos supports the automated reverse engineering of binaries with an emphasis on malicious code analysis," said the SEI's Cory Cohen. "It reduces malware analysis from hours to seconds so analysts can keep up with adversaries." The tool can also be used to analyze trusted software code.

Automating Vulnerability Discovery with BFF and SMART

By delivering and improving automated vulnerability discovery techniques, SEI researchers can increase the DoD's assurance in the software it uses. Two SEI-developed tools aim to do just this:

- Basic Fuzzing Framework (BFF) finds defects in applications by performing mutational fuzzing on software that consumes file input.
- Synergistic Mayhem AFL Research Tool (SMART) performs automated, high-coverage vulnerability discovery on binary file-parsing software, combining a mutational fuzzer with a binary concolic (concrete and symbolic) executor to generate new test cases.

"BFF and Smart use dynamic binary analysis," said the SEI's Ed Stoner, "which means the analysis can take place while the software is running and without requiring source code."

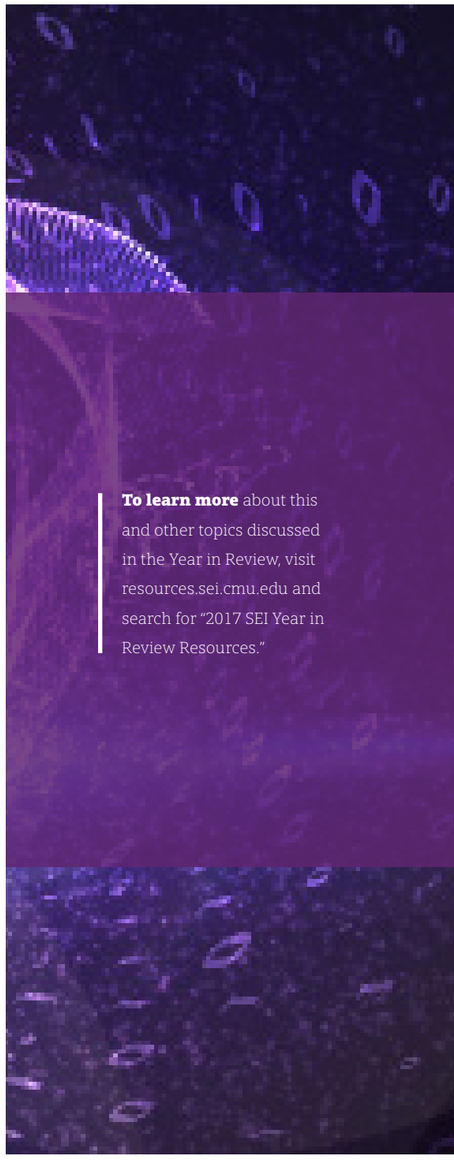
Automated Code Repair

Many security bugs follow common patterns, and often there is a corresponding pattern for repair. SEI secure coding researchers are developing tools to automatically remediate such vulnerabilities. Recent work centers on vulnerabilities related to integer overflow and memory bounds.

"We devised and implemented an approach that automates how memory-sensitive integer overflow is detected and repaired," said the SEI's Will Klieber. In this approach, an arithmetic operation is memory sensitive if it is used to calculation of how much memory to allocate or an inequality comparison involving the bounds of an array.

"Our team is also investigating techniques for inferring the bounds of memory that should be accessible via given pointers," noted Klieber. Bounds checks can prevent invalid writes (which can corrupt memory) and invalid reads (which can leak sensitive information). "We're using static analysis to propose candidate bounds," explained Klieber, "weeding out too-strict candidate bounds using dynamic analysis and repairing the program by inserting code that checks the bounds."

Projects like these exemplify the ways SEI researchers are working to help the DoD improve malware response, find vulnerabilities, and acquire and develop conforming software. As threats increase and attackers become more sophisticated, SEI researchers develop and share ideas, collaborate, and extend their research to produce strategies, tools, and advice that help the DoD protect its networks and data.



To learn more about this and other topics discussed in the Year in Review, visit resources.sei.cmu.edu and search for "2017 SEI Year in Review Resources."

Researcher

JEFF BOLENG

Bringing Modern Software Development Practices to the DoD

"Software and system complexity is increasing software cost and software vulnerability," says Jeff Boleng, chief technology officer (acting) and deputy CTO for the SEI. "At the same time, more and more system capability results from software, which will evolve over the lifetime of the system. This situation jeopardizes military capability."

Certainly, the software challenges facing the Department of Defense (DoD) are serious, and the stakes are high. Software cost overruns are overwhelming program delivery and sustainment. Hidden vulnerabilities and those exposed during operations are putting the DoD at risk. Finding and fixing problems late in the application lifecycle are driving up costs and delaying deployment, putting missions at risk. Manual and lengthy deployment processes lead to delayed response to any possible security incident or patch to zero-day vulnerabilities.

To move forward on these challenges, the adoption of modern software development practices and automated tools is a must. Certainly, nudging a large, complex organization into new ways of doing things can be tough, and the DoD faces numerous impediments to modernization, including risk acceptance, acquisition policy, slow adoption of open standards, and long delivery cycles. But progress is possible, and the SEI has been at work helping the DoD adopt modern software development practices for several years.

Agile

One area in which the SEI is making great strides is in research and development on the use of Agile practices in the DoD's large-scale environment. Working closely with DoD and government organizations, the SEI has examined areas in which Agile makes sense, applying Lean approaches to enable the scaling demanded by complex enterprises and systems.

The SEI has paid special attention to the ways in which the DoD needs to tailor oversight functions, insight, and technical milestone reviews. It has also highlighted the ways in which adoption is facilitated through leadership buy-in, the adaptation of process to suit specific environments, and workforce development programs. The result? Many programs adopting Agile approaches are reporting improvements in cost, engagement and collaboration, and quality.

To help foster understanding and adoption of Agile approaches in DoD and government settings, the SEI has engaged with the community in a number of important ways. For instance, the SEI leads a unique Agile Collaboration Group, whose membership exceeds 200 individuals representing more than 65 organizations across government, industry, and academia, all of whom share an interest in transitioning Agile approaches to the DoD and other highly regulated settings.

The group has worked with the Defense Acquisition University to incorporate Agile concepts into the DoD's professional acquisition curriculum. It launched an annual Agile Colloquium for DoD and federal government Agilists. It also engaged with the Section 809 panel charged with streamlining and improving the defense acquisition process. And it has briefed leadership in the DoD, the services, and the House Ways and Means Subcommittee on Social Security.

A series of webinars, blog posts, and technical reports and other publications represent some of the assets developed to aid in transitioning Agile approaches to the DoD and federal acquisition communities.

DevOps

DevOps emphasizes communications, collaboration, automation, and continuous integration among software developers and information technology operations personnel. It works hand in glove with Agile. The SEI has been a leader in DevOps research and development, particularly with regard to its application in the DoD.

The SEI has been looking at ways to tailor DevOps principles to program needs and implement tailored development pipelines. It's also researched the application architectures that enable iterative and incremental developments; the integration of continuous security throughout the development pipeline; and integrating compliance into the DevOps development pipeline. To help evangelize DevOps, the SEI was a key participant in All Day DevOps, the first global, online DevOps conference, which launched in 2016. It has also produced technical reports detailing SEI DevOps research and a dedicated blog to promote the latest thinking on all matters DevOps. The SEI engages with the DevOps community at various conference venues by delivering talks or workshops, and it is actively involved in IEEE DevOps standards development.

Modern Deployment Tools Chain

The third leg in this effort is a modern deployment tools chain on an integrated development pipeline. Software automation and factory tooling make it easier to move to a continuous development, test, and delivery model. But significant challenges present several barriers—such as air-gapped environments and authority to operate processes—to adopting a modern deployment tools chain in the DoD. The SEI is beginning to examine these challenges. How should the pipeline be engineered? Who will own it? How will it be monitored and assessed? What attributes and requirements need to be addressed when selecting tools to be integrated to the pipeline? How can all stakeholders be included in the application lifecycle on an automated and integrated development pipeline?

Agile, DevOps, and the software factory integrated deployment tools chain enable technologies for the DoD's competitive advantage. These technologies include autonomous systems, automated code generation, deployment and repair, and artificial intelligence. They also drive new challenges and the need for fresh research and development, including research in the area of human–system trust, continuous runtime assurance, new testing regimens, and software maintenance and evolution. The SEI is hard at work in all these areas, helping to bring modern software development practices to the DoD.

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

"Our focus is the most complex of today's systems, such as weapon and control systems, applying a wide range of software analyses and data analytics."

—JOHN BRAMER, DIRECTOR (ACTING), SOFTWARE SOLUTIONS DIVISION

CMU Leadership

President (Interim)
FARNAM JAHANIAN

Provost (Interim)
LAURIE R. WEINGART

SEI Executive Leadership

From left: Daniel Bauer, Director of Talent Management; John Bramer, Director (Acting), Software Solutions Division, Chief of Staff; Jeff Boleng, Chief Technology Officer (Acting) and Deputy CTO; Mary Catherine Ward, Chief Strategy Officer; Peter Menniti, Chief Financial Officer; Bobbie Stempfley, Director, CERT Division; Paul Nielsen, Director & Chief Executive Officer; Robert Behler, Chief Operating Officer; Sandra Brown, SEI General Counsel; David Thompson, Chief Information Officer; Matthew Gaston, Director, Emerging Technology Center

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

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

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

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

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

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

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

Donald Stitzenberg
Chair, Board of Visitors; Consultant; Former Assistant Director, MIT Lincoln Laboratory

SEI Leadership

DIRECTOR'S OFFICE

Paul D. Nielsen
Director & Chief Executive Officer

Jeff Boleng
Chief Technology Officer (Acting) and Deputy CTO

Robert Behler
Deputy Director and Chief Operating Officer

SOFTWARE SOLUTIONS DIVISION

John Bramer
Director (Acting)

Anita Carleton
Deputy Director

Charles Holland
Chief Scientist

EMERGING TECHNOLOGY CENTER

Matthew Gaston
Director

Brenda Penderville
Deputy Director (Acting)

CERT DIVISION

Bobbie Stempfley
Director

Bill Wilson
Deputy Director

Greg Shannon
Chief Scientist

OFFICES OF THE CHIEF OF STAFF/ CHIEF INFORMATION OFFICER

Roman Danyliw
Chief Engineer

John Bramer
Chief of Staff

David Thompson
Chief Information Officer

FINANCIAL & BUSINESS SERVICES

Peter Menniti
Chief Financial Officer

STRATEGIC INITIATIVES

Mary Catherine Ward
Chief Strategy Officer

SEI LEGAL

Sandra Brown
SEI General Counsel

Copyright

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.

DM17-1018

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
Claire Dixon
Tamara Marshall-Keim
Gerald Miller
John Morley
Nancy Ott
Sandy Shrum
Barbara White

Technical Advisor to the Director and CEO
Ryan Meeuf

Design
Christopher Baum

Illustration
Kurt Hess

Digital Production
Mike Duda

Photography
David Biber
Tim Kaulen, Photography and Graphic Services, Mellon Institute

SEI Pittsburgh, PA

4500 Fifth Avenue
Pittsburgh, PA 15213-2612

SEI Washington, DC

Suite 200
4301 Wilson Boulevard
Arlington, VA 22203

SEI Boston, MA

One Burlington Center
67 South Bedford Street
Suite 400W
Boston, MA 01803

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

SEI San Antonio, TX

AFLCMC/HIH
1960 First St. West
Bldg. 977C, Room C208
JBSA-Randolph, TX
78150-4453