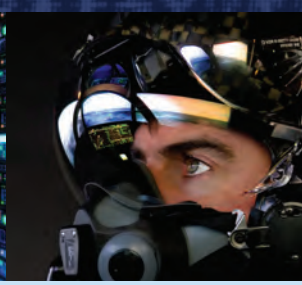
2014 | YEAR IN REVIEW

Photo: U.S. Army/Michael L. Lewis/Released



Software Engineering Institute
Carnegie Mellon University

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.

Message From the Director

In 1988, the interdependence between software and cybersecurity crystallized when the Morris worm compromised about 10 percent of all systems connected to the fledgling internet. The Morris worm revealed that the cyber environment, though powerful, was also susceptible to attack. DARPA, the defense research agency behind the internet, responded to the attack by funding the CERT Coordination Center® at our Carnegie Mellon University (CMU) Software Engineering Institute (SEI).

Since then, the CERT mission has grown beyond incident response. In 2014, we celebrated the CERT® Division's 25 years of leadership in R&D for vulnerability discovery, malware analysis, insider threat, secure coding, operational resilience, and workforce development. IEEE has taken note of CERT contributions and in 2014 named Dr. Greg Shannon, CERT chief scientist, as head of its Cybersecurity Initiative.

SEI work in software-related security and engineering issues fosters the creation of more reliable, secure, and enduring systems, and it supports continuing cost and schedule improvement in acquisition. In 2014, we expanded our R&D footprint by establishing the Empirical Research Office (ERO) and the Cyber Intelligence Research Consortium (CIRC). The ERO will spearhead research to provide the Department of Defense (DoD) the data it needs to improve its software acquisition, development, and sustainment practices. Through the member-funded CIRC, organizations will benefit from innovative solutions and practices to help them make better decisions about cyber intelligence. We also provided expertise directly to DoD and government agencies in more than 150 engagements, and we collaborated with fellow FFRDC MIT Lincoln Laboratory to address DoD and national security challenges. In addition, we developed and implemented new training programs to build skills in combatting cybersecurity insider threats.

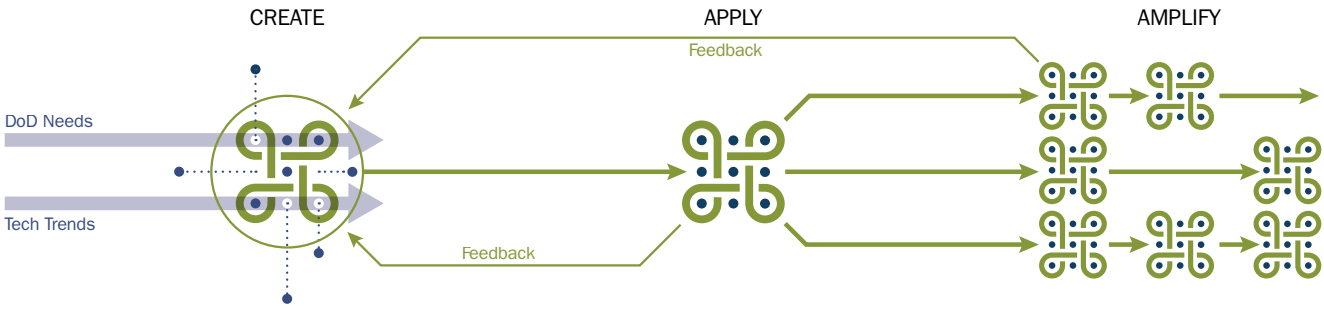
Along the way, we created new opportunities for our stakeholders to learn about the value of our forward-looking software and cybersecurity research. At our two 2014 Research Review events, our principal researchers presented current projects to stakeholders and discussed the practical uses of our work.

As our work in 2014 again showed, the SEI engages successfully with the software and cyber communities important to the nation's security, fostering productive collaborations and leading the broad adoption of dramatic improvements in practice.

Paul D. Nielsen
Director and CEO

Strategy

The SEI achieves its goals through technology, innovation, and transition. The SEI creates usable technologies, applies them to real problems, and amplifies their impact by accelerating broad adoption.



CREATE

The SEI addresses significant and pervasive software engineering and cybersecurity problems by

- motivating research
- innovating new technologies
- identifying and adding value to emerging or underused technologies
- improving and adapting existing solutions

SEI technologies and solutions are suitable for application and transition to the software engineering and cybersecurity communities and to organizations that commission, build, use, or evolve systems that are dependent on software. The SEI partners with innovators and researchers to implement these activities.

APPLY

The SEI applies and validates new and improved technologies and solutions in real-world government and commercial contexts. Application and validation are required to prove effectiveness, applicability, and transition potential. Solutions and technologies are refined and extended as an intrinsic part of the application activities.

Government and commercial organizations directly benefit from these engagements. In addition, the experience gained by the SEI informs

- the “Create” activities about real-world problems and further adjustments, technologies, and solutions that are needed
- the “Amplify” activities about needed transition artifacts and strategies

The SEI works with early adopters to implement the “Apply” activities.

AMPLIFY

The SEI works through the software engineering and cybersecurity communities and organizations dependent on software to encourage and support the widespread adoption of new and improved technologies and solutions through

- advocacy
- books and publications
- courses
- leadership in professional organizations
- licenses for use and delivery
- web-based communication and dissemination

The SEI accelerates the adoption and impact of software engineering and cybersecurity improvements.

The SEI engages directly with the community and through its partners to amplify its work.

Areas of Work

Software is critical to the system capabilities the Department of Defense (DoD) needs to achieve its mission. The pace of innovation in information technology (IT) is unmatched by any other technology crucial to the DoD's mission readiness and success. The expectations placed on software and IT have only increased. If the DoD is to acquire and deploy trustworthy software-enabled capabilities, it must address systems engineering, cybersecurity, and software engineering together from conception to sustainment.

Since 1984, the Software Engineering Institute (SEI) has served the nation as a federally funded research and development center sponsored by the DoD. The SEI helps organizations improve their ability to acquire, develop, operate, and sustain software systems that are innovative, affordable, enduring, and trustworthy.

The SEI conducts research and development and publishes findings in these areas, and works together with partners and collaborators in industry, academia, and government. The SEI also undertakes pilot programs to refine best practices and inform our future technical direction. The SEI disseminates mature and proven solutions through software tools, training courses, licensing, and publication of best practices.

To support these objectives, the SEI focuses on several technical directions in the following major areas:

Software Engineering, including issues of software system acquisition, design, development, integration, testing, sustainment, and measurement

Cybersecurity, including activities related to the security of networks and computers, with a strong focus on deployable tools, methods, and workforce development

Assurance, comprising a combination of techniques in software engineering and security that focus on a "designed-in" approach throughout the software lifecycle

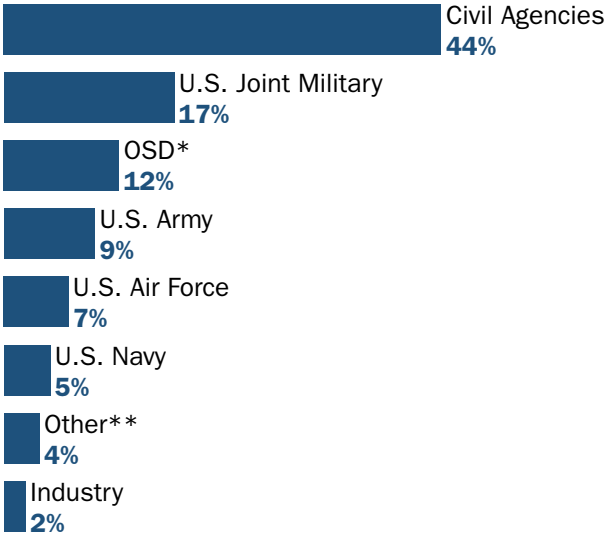
DoD Critical Component Capabilities, such as cyber-physical systems, high-performance computing and parallel algorithms, mobile applications, networking, and autonomous operations

Funding

In FY 2014, the SEI received funding from a variety of sources in the Department of Defense, civil agencies, and industry.

* funding provided by the Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics—the SEI's primary DoD sponsor—to execute the SEI technical program

** course fees, conference fees, and other recovered costs



SEI's CERT Division Marks 25 Years of Service

The SEI's CERT Division traces its roots to 1988 when, in the wake of the Morris worm incident, DARPA charged the SEI with establishing a capability to coordinate response during computer security emergencies and build awareness of security issues across the internet community. On December 12, 1988, the original team of one SEI staff member, one administrative assistant, and three part-time members borrowed from the IT department, received its first reported security incident. The CERT Division has never been without an active incident since.

Today, more than 25 years later, the CERT Division is a national asset in the field of cybersecurity. Its mission has grown well beyond incident response to include research and development in the areas of vulnerability analysis, secure coding, network situational awareness, insider threat, cybersecurity engineering, workforce development, and other related fields. The CERT Division's present staff of more than 250 is widely recognized as a trusted, authoritative organization dedicated to improving the security and resilience of computer systems and networks. It regularly partners with government, industry, law enforcement, and academia to develop advanced methods and technologies to counter large-scale, sophisticated cyber threats.

To learn more about the SEI's CERT Division, visit http://www.cert.org.

Multi-Year Collaboration with DOE Nets Advances in Cybersecurity Assessment


Jim Cebula


Nader Mehravari

"C2M2 is quick, efficient, and cost effective. It serves as an effective starting point for organizations to identify trouble spots that warrant further diagnosis."

—Jim Cebula

For several years, the SEI has collaborated with the Department of Energy (DOE) and other stakeholder organizations to reduce the risk of energy disruptions and improve the electric power grid's ability to withstand and respond to cyber incidents. As part of this effort, the SEI served as the model architect for the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2). Funded by the DOE, ES-C2M2 was developed as part of a White House initiative to enhance the security and reliability of the nation's electrical grid. Published in 2012, the ES-C2M2 methodology and its self-evaluation tool allows utilities and grid operators to assess their cybersecurity capabilities and prioritize their efforts to improve cybersecurity.

Building on that success, in 2013 the SEI continued its work with the DOE to produce a new, more generic cybersecurity methodology (known as C2M2). This generic model grew out of the great interest in ES-C2M2, and it facilitated further adaptation beyond the electricity subsector. As model architect, the SEI worked closely with the DOE to draw on the body of knowledge contained in the SEI's CERT® Resilience Management Model (CERT® -RMM).

"C2M2's lightweight assessment tool provides what we call *maturity indicator levels*," said Jim Cebula, the SEI's technical manager on the project. Cebula explained C2M2 is designed to be executed in a short period of time and to give organizations indicators of the maturity of their operational capabilities and their ability to manage cybersecurity risk. "C2M2 is quick, efficient, and cost effective," said Cebula. "It serves as an effective starting point for organizations to identify trouble spots that warrant further diagnosis."

The success of ES-C2M2 and the release of C2M2 spurred interest in the model from the oil and gas subsector, which led to the development of a new subsector-specific model (ONG-C2M2), which was published in early 2014.

All of this activity drew the attention of the DOE's Office of the Chief Information Officer (DOE CIO). "The DOE CIO approached us this year and suggested that the C2M2 concept was applicable not just to energy domains, but to any IT service delivery organization," said the SEI's Nader Mehravari. With funding from the DOE CIO, Mehravari headed a development team that produced C2M2 for IT Services.

The SEI conducted a pilot of C2M2 for IT Services at a DOE IT facility. "This was the third time we developed and piloted a C2M2-based model," said Mehravari. The team's past experience helped it draft a methodology nearly ready for prime time. "We had no surprises," said Mehravari, "and practically no major requests for change after the pilot."

To date, downloads of the C2M2 toolkit have numbered in the hundreds, a number that indicates significant interest in the energy sector and other sectors.

In addition to its work on C2M2 and derivative products, the SEI team helped develop guidance for organizations working to implement the National Institute for Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity. "The guidance explains the ways organizations can use C2M2 to meet the goals and objectives of the NIST framework," said the SEI's James Stevens, an SEI contributor to the NIST guidance document.

Stevens noted the team's work is not done. In the coming fiscal year, the SEI will contribute to the next version of the C2M2 model. "We also plan to build on lessons learned from using the C2M2 products," said Stevens. "The development of the model will continue to include participation from energy sector stakeholders."

For more about the SEI's work on C2M2, visit http://www.cert.org/podcasts/podcast_episode.cfm?episodeid=81836.

SEI Expertise Supports the U.S. Army's Joint Multi-Role Technology Demonstrator Effort

Software for mission- and safety-critical systems, such as avionics systems in aircraft, is growing larger and more expensive. Software now accounts for two-thirds of the total system cost. A 2002 study by the National Institute of Standards and Technology revealed that the majority of software system problems are introduced during requirements specification and architecture design but are not discovered until after unit testing. These concerns are of utmost importance to U.S. Army personnel leading the Joint Multi-Role Technology Demonstrator (JMR TD) effort and Future Vertical Lift (FVL) initiative. The purpose of the JMR TD is to demonstrate transformational vertical lift capabilities to prepare the Department of Defense (DoD) for decisions regarding the replacement of the current vertical lift fleet while reducing risk for transition to the FVL. Both efforts play key roles in the development of the DoD's next-generation rotorcraft fleet.

To address the early development concerns of these programs, the Army has funded work on architecture modeling with the Architecture Analysis and Design Language (AADL), and the SEI is the technical lead. This technology has been shown to discover problems early in the software development lifecycle through virtual system integration and analysis. It helps reduce cost and decrease certification time by enabling developers to perform assurance activities more effectively throughout the lifecycle of the system.

JMR has embraced this technology and dubbed it the "architecture-centric virtual integration process," or ACVIP. A team consisting of Bruce Lewis (U.S. Army Aviation and Missile Research, Development, and Engineering Center Software Engineering Directorate, or AMRDEC SED), Peter Feiler (SEI), and Steve Vestal (Adventium Labs) developed a technology roadmap for the maturation and adoption of ACVIP and briefed JMR Program Director Dan Bailey, who subsequently discussed the strategy at a Center for Strategic and International Studies panel titled "Common Architectures for Future Rotorcraft," describing it as "the DoD version of what the SAVI [System Architecture Virtual Integration] group has been working on for years" in the aerospace industry.

In 2014, the SEI team of Feiler and colleague John Hudak, with collaborator Adventium Labs, employed a prototype of ACVIP to shadow a JMR project in which an AMRDEC team integrated data correlation and fusion systems from two contractors into a laboratory-based aircraft survivability infrastructure. The SEI team mapped the stakeholder- and system-requirement documents into a system-requirement specification associated with an AADL model. By analyzing the resulting AADL model, the team quickly discovered a range of ambiguity and inconsistency issues in the original documents. Significantly, the team found these potential issues early in the development process, before the system was built.

Second, the SEI team discovered potential system-integration problems. When the team performed a safety analysis, it found that the requirements specifications had imposed architectural decisions that would interfere with the system's response time. "People do not usually see this effect until they put the system together, run it, and start measuring," noted Feiler. The Adventium team also performed global timing analysis on the resulting system based on data from contractors.

JMR found the results of the ACVIP shadow project important enough to share with contractors, and the JMR program team now plans to recommend that contractors use this technology in the next phase of demonstrations.

To learn more about the SEI's work in AADL, visit
http://www.sei.cmu.edu/architecture/research/model-based-engineering/aadl.cfm.

Photo courtesy of U.S. Army

Peter Feiler

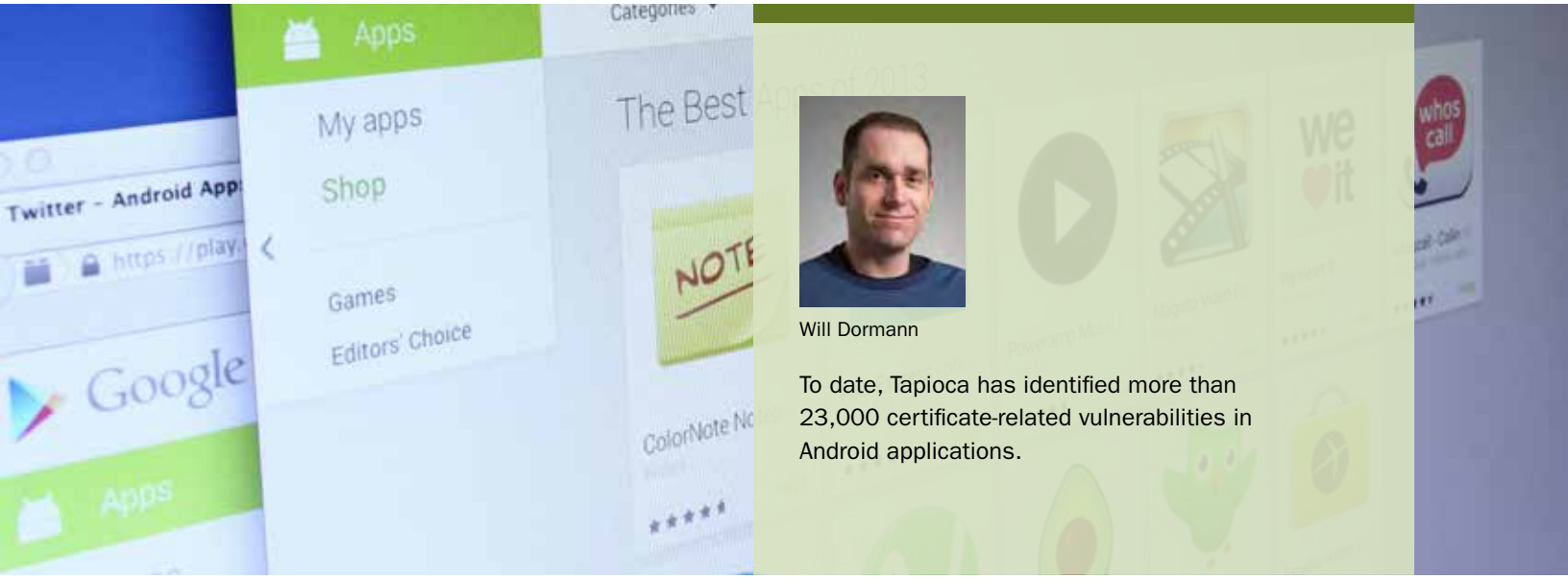
"AADL helps reduce cost and decrease certification time by enabling developers to perform assurance activities more effectively throughout the lifecycle of the system."

—Peter Feiler

AMRDEC is part of the U.S. Army Research, Development and Engineering Command, which has the mission to develop technology and engineering solutions for America's soldiers. AMRDEC employs nearly 11,000 civilian scientists, researchers, and engineers.

The Research, Development, and Engineering Command (RDECOM) is a major subordinate command of the U.S. Army Materiel Command. AMC is the Army's premier provider of materiel readiness—technology, acquisition support, materiel development, logistics power projection, and sustainment—to the total force, across the spectrum of joint military operations.

CERT's Tapioca Identifies Apps Vulnerable to Man-in-the-Middle Attacks



Will Dormann

To date, Tapioca has identified more than 23,000 certificate-related vulnerabilities in Android applications.

Will Dormann, a vulnerability analyst with the SEI's CERT Division, made a small discovery in 2014 that netted significant information about the security of Android smartphone apps. Investigating network traffic generated by software applications, Dormann needed a transparent man-in-the-middle (MITM) proxy that operated at the network layer. Available tools operated only at the application layer.

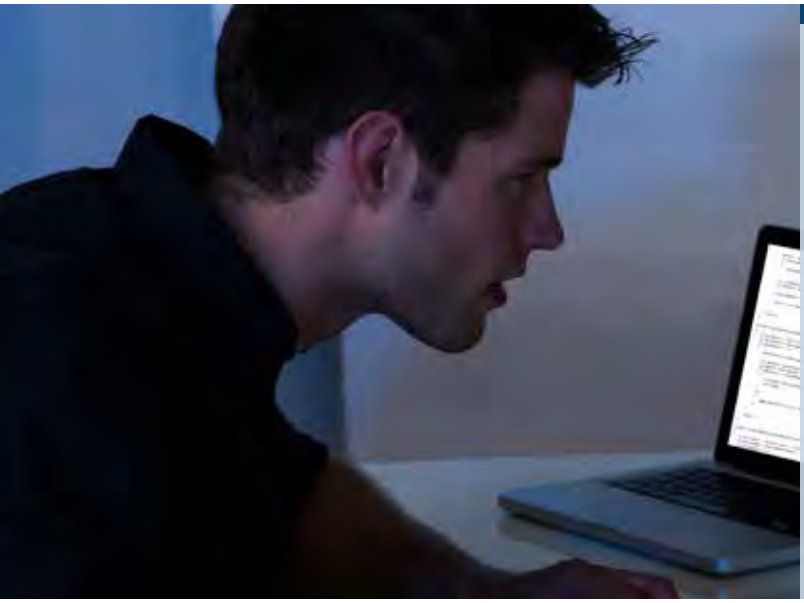
"After a bit of trial-and-error," said Dormann, "I found a software combination that did the trick." He dubbed the result "Tapioca," shorthand for Transparent Proxy Capture Appliance. Tapioca is a network-layer MITM proxy virtual machine that combines the CERT Division's UbuFuzz virtual machine with the tool mitmproxy. "Because Tapioca operates at the network layer," noted Dormann, "I can transparently test applications and devices that do not support proxies." Tapioca can investigate all HTTPS traffic generated by applications and, importantly, it can check for applications that fail to validate SSL certificate chains.

Dormann tested Tapioca on a handful of Android apps. The results were encouraging but, at 60 seconds per test, time consuming. For instance, to test all the apps available through Google Play would have taken Dormann eight years. To address this problem, Dormann worked to automate Tapioca, and the results have been impressive. In 2014, the CERT Division applied Tapioca to wide-scale testing of Android apps, made it a policy to notify the author of every application that failed Tapioca testing, and provided them guidance on remediating the problem. It also published a growing list of affected apps, providing end-users information they need to take appropriate action.

To date, Tapioca has been used to test approximately 1 million apps and has identified more than 23,000 certificate-related vulnerabilities in Android applications.

To learn more about how the SEI's CERT Division is using Tapioca to detect Android vulnerabilities, visit https://www.cert.org/vulnerability-analysis/tools/cert-tapioca.cfm.

SEI Forms Cross-Sector Group to Advance the Practice of Cyber Intelligence



Jay McAllister, Samantha Allen, Melissa Ludwick

Sound cyber intelligence practices enable the prevention and mitigation of security breaches. This is why the SEI's Emerging Technology Center (ETC) partners with public and private sector organizations to research cyber intelligence methodologies, processes, technologies, and training. To spur further development and improve capabilities in these areas, the SEI launched the Cyber Intelligence Research Consortium in June 2014.

"Recent highly publicized security breaches reinforce the importance of cyber intelligence for any organization, regardless of size and economic sector," said Jay McAllister, an ETC senior analyst and technical lead of the consortium. "But many organizations operate without a research-verified set of practices. The consortium exists to help organizations determine how best to excel in this emerging discipline."

Cyber Intelligence Research Consortium members identify challenges involving the art and science of applying knowledge to information to produce intelligence. Consortium staff members then address these challenges in numerous in-person and virtual offerings. These offerings include developing newsletters and how-to guides on effective analytical methodologies, evaluating intelligence, and assessing the critical thinking and problem-solving skills needed to analyze cyber threats. Future offerings will involve member participation in a workshop showcasing relevant technologies and a crisis simulation created to hone technical and strategic analytical skills.

The consortium's membership currently includes American Express, PNC Bank, Wells Fargo, Dominion Energy, Carnegie Mellon University, AirBus, and organizations from the U.S. intelligence community and military. New members may join at any time.

For more information on the SEI's Cyber Intelligence Research Consortium, visit http://www.sei.cmu.edu/about/organization/etc/overview.cfm**.**

SEI's Client Technical Solutions Staff Crafts Technical Solutions for Government and DoD Organizations

2014 was another year of multiple successes for SEI Client Technical Solutions (CTS) in providing direct help to government-sponsored IT and software engineering programs. In providing this assistance, our members of the technical staff frequently applied SEI-developed tools, techniques, and capabilities in the everyday working environments of the organizations the SEI serves. The following projects highlight a small sample of the work undertaken by CTS staff in support of our sponsor organizations.

Acquisition Support for the Air Force's Con-IT
The SEI provided valuable data the Air Force will use to prepare for a new, major acquisition called Contracting Information Technology (Con-IT). The Air Force Con-IT team is acquiring and deploying an enterprise-wide contract preparation and management capability, and it relied on the SEI to examine and analyze existing capabilities and options for building the system. The SEI, working with the Air Force team and employing SEI analysis techniques and expertise, examined existing systems and architecture artifacts, performed a detailed review and revision of the Con-IT non-functional requirements, and delivered a detailed market analysis of leading enterprise IT commercial off-the-shelf (COTS) solutions.

"In an unstable economic environment rife with austere budgets, the Air Force must make every dollar count," said Joseph Matis, the Con-IT program manager. "Using the SEI proved instrumental in helping the Air Force perform due diligence on current technologies—thus reducing the amount it would have invested in prototyping technologies that could not meet the demanding warfighter requirements."

Support for Marine Corps Data Network Modernization
The SEI also enjoyed success in 2014 with the Marine Corps Global Combat Support System (GCSS-MC)—the system that handles logistics across the Marine Corps. GCSS-MC rides on the existing Marine Corps Data network and substantially improves the combat effectiveness of the Marine Air Ground Task Force (MAGTF).

"We're helping the Marine Corps make decisions about how best to modernize the core enterprise system," said Steve Beck, the SEI team's lead. "The idea is to create an enterprise system that is vendor friendly—that is, one that all system and software vendors can fit their products into and be compatible with."

Working with the Marine Corps project team, the SEI looked at multiple technologies, analyzed them, and made recommendations to the Marine Corps leadership. A team of more than a dozen SEI staff worked on the project, including Beck, John Robert, Donald Beynon, Carol Connelly, Robin Eisenhart, Lover Epps, Donald Firesmith, Debra Lange, Harry Levinson, Craig Lewis, Laura Machione, Jay Marchetti, Gerald Miller, Colleen Regan, Chrissie VanTol, and Michael Zuccher. "The impact of what is being done now will be felt for 20 years," Beck said, noting that "nothing happens without logistics."

Photo courtesy of U.S. Marine Corps.


Stephen Beck


Julie Cohen


Mike Bandor

The Office of Medicare Hearings and Appeals (OMHA**):** The SEI helped OMHA replace a paper appeals process with a commercial off-the-shelf electronic system that will facilitate an electronic case adjudication and processing environment, including an electronic case file. The SEI reviewed the request for proposal for the new system and produced a key data quality report, said SEI team lead Julie Cohen.

The Predator/Reaper program: The SEI is helping to establish a metrics program for the MQ-9 and MQ-1 systems that control unmanned aircraft. SEI technical lead Mike Bandor said the metrics program "provides meaningful information to the government for both acquisition and sustainment" of the Predator and Reaper systems.

SEI Teams with MIT Lincoln Laboratory on Critical DoD Problems

The SEI has teamed with the Massachusetts Institute of Technology (MIT) Lincoln Laboratory to harness the strengths of the two research and development centers. The SEI provides the technical leadership needed by the DoD to advance technologies and practices to acquire, develop, operate, and sustain software systems that are innovative, affordable, trustworthy, and enduring. The core work of Lincoln Laboratory focuses on sensors, signal processing and embedded computing, communications, and integrated sensing and decision support, all supported by a broad research base in advanced electronics.

"The SEI and Lincoln Laboratory are both working toward the same overarching goal: to solve problems that are critical to the DoD and national security," said the SEI's Anita Carleton, deputy director, Software Solutions Division. "Working together allows us to leverage our strengths toward comprehensive solutions for the DoD. We bring more than 25 years of experience in software and cybersecurity, while Lincoln Laboratory draws on more than 60 years of unmatched research expertise in advanced systems, sensors, processing, decision support, and prototyping."

To help Lincoln Laboratory meet its objectives for its sponsoring organizations, the SEI collaborated to:

- perform architecture discovery, assessment, and documentation of a cybersecurity analysis big data application. The SEI also composed models of cyber systems under different defender and adversary conditions, and integrated them into a modeling and simulation framework. Lincoln Laboratory's cyber modeling and simulation capability is used to simulate defensive mitigations for cyber attacker, user, and defender scenarios.
- improve the stability of a situational awareness platform. The SEI helped collect and document hardware and software architecture system specifications along with end-user workflows and primary use cases for the Lincoln Laboratory project, and provided prioritized recommendations to meet end user needs.
- estimate sustainment costs of an agile, net-centric architecture used to deliver common tools and capabilities across a large enterprise network. The SEI helped collect and document effort against existing system and software engineering processes, including sustainment goals that enable effective transition to customers, architecture and design documentation, and better understanding of development and maintenance costs.
- support the evaluation of data-integrity-related technologies that may be applicable to a Lincoln Laboratory client. As part of this work, the SEI assessed and validated the data integrity architecture for the platform and provided prototypes for data-integrity-related analytics.

"This collaboration allows experienced SEI researchers to share software and cybersecurity expertise with Lincoln Laboratory's research and development programs," said Scott Hissam, a principal researcher at the SEI. "Specifically, the SEI is helping them enhance software prototyping and development processes to support the production of high-quality, sustainable, and operationally readied capabilities for warfighters."

Photo courtesy of MIT Lincoln Laboratory.


Anita Carleton

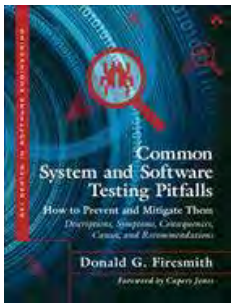

Scott Hissam

"Working together allows us to leverage our strengths toward comprehensive solutions for the DoD. We bring more than 25 years of experience in software and cybersecurity, while Lincoln Laboratory draws on more than 60 years of unmatched research expertise in advanced systems, sensors, processing, decision support, and prototyping."

—Anita Carleton

Better Testing Makes Better Software: SEI Book Helps Testers Avoid Pitfalls

Donald G. Firesmith

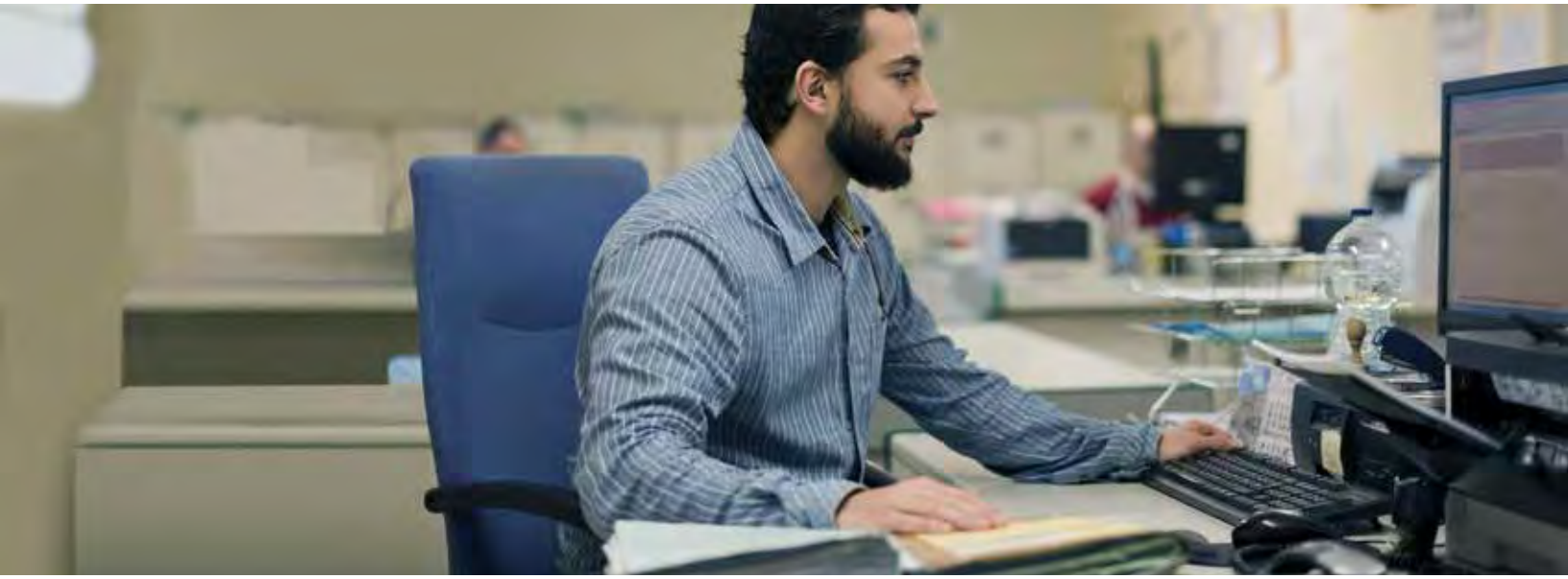


For SEI Principal Engineer Donald G. Firesmith, 2014 saw the publication of Common System and Software Testing Pitfalls: How to Prevent and Mitigate Them, the latest in Addison-Wesley's SEI Series in Software Engineering. Written primarily for software testers and their technical managers, the book helps readers recognize, avoid, and mitigate potential testing-related pitfalls. It also helps system stakeholders gain a better understanding of what can go wrong with testing. Software engineering luminary Capers Jones wrote that the book "is likely to become a standard for test training as well as a good reference for professional testers and developers."

Firesmith's work documents 92 pitfalls, including potential symptoms, consequences, causes, and recommendations. Since its publication, further research has grown the associated repository to 167 pitfalls in 23 categories. Firesmith, with 36 years of industry experience, is an internationally recognized subject matter expert who has published seven software and systems engineering books in the areas of requirements engineering, architecture engineering, situational method engineering, testing, and object-oriented development.

For more information, visit http://blog.sei.cmu.edu/post.cfm/common-testing-problems-pitfalls-to-prevent-and-mitigate.

Self-Assessment Package Provides New Option for Measuring Resilience



Since 2009, more than 400 organizations have examined their preparedness to handle disruptive cyber events through the Cyber Resilience Review (CRR). This assessment method measures essential cybersecurity capabilities and behaviors that indicate an organization's operational resilience during normal operations and times of operational stress.

The CRR was created by the SEI's CERT Division in collaboration with the Department of Homeland Security (DHS), whose facilitators deliver it through an eight-hour workshop. It comprises 271 questions across 10 domains of capability in critical infrastructure organizations.

The CRR is derived from the CERT Resilience Management Model (CERT-RMM), developed by the SEI. A capability-focused maturity model for process improvement, it reflects best practices from industry and government for managing operational resilience.

In 2014, CERT developed the CRR Self-Assessment Package, which allows organizations to apply the CRR method without the participation of external facilitators. It contains the same questions, scoring mechanisms, and options for improvement as the externally facilitated CRR. The CRR Self-Assessment enables an organization to assess its capabilities relative to the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF).

The self-assessment package includes a crosswalk document that maps the CRR to the NIST CSF. An implementation guide aids in conducting the self-assessment, interpreting the self-assessment report, and making improvements in cybersecurity practices.

Organizations considering the CRR or CRR Self-Assessment can explore resilience concepts through the Cyber Resilience Workshop, recently developed by DHS in partnership with the SEI.

For more information on the CERT Division's work on resilience management, visit http://www.cert.org/resilience.

Emerging Technology Center Helps Set National Priorities for Cyber Research

Matt Gaston

"We bridge the gap to the outside world. We bring in the best ideas from everywhere."

—Matt Gaston

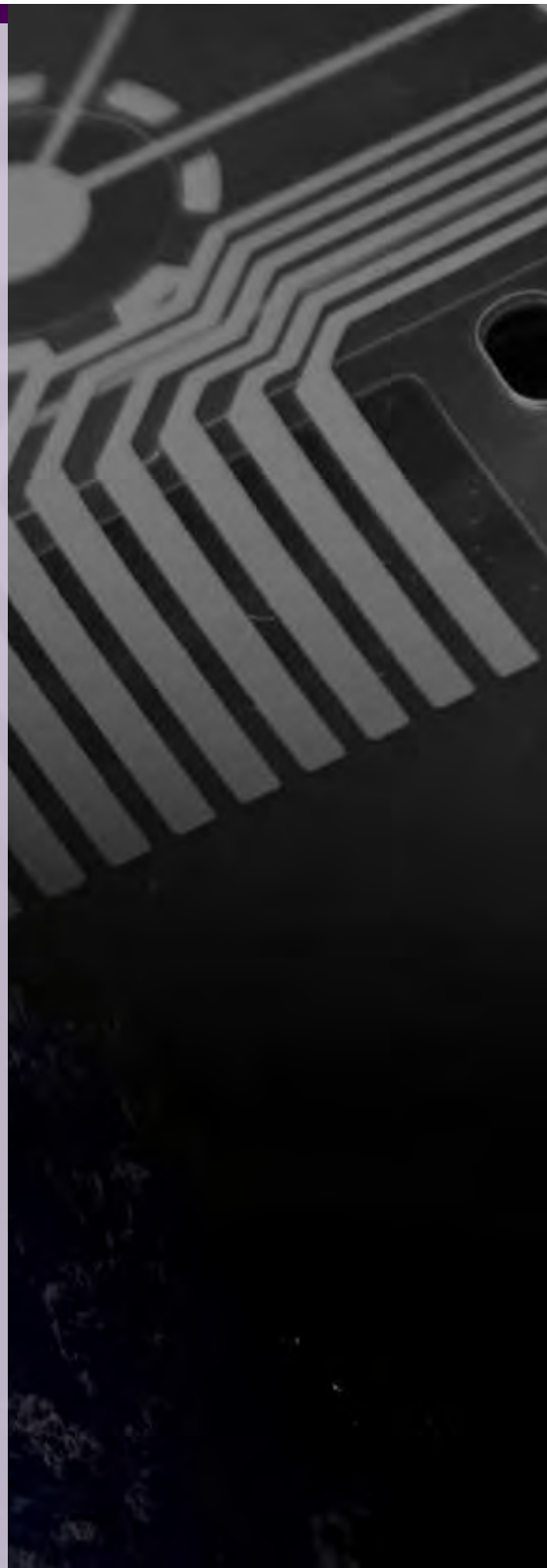
The SEI's Emerging Technology Center (ETC) is lending its expertise to chart a path for the U.S. intelligence community's cyber research priorities. In support of the Special Cyber Operations Research and Engineering (SCORE) Working Group, the ETC provides thought leadership and identifies emerging trends and opportunities for research.

SCORE, an interagency working group, was established in 2008 with oversight by the White House Office of Science and Technology Policy. With representatives from about 20 government organizations, SCORE promotes collaboration, awareness, and priority setting.

The ETC began supporting SCORE in January 2014, shortly after the annual SCORE Computational Cybersecurity in Compromised Environments (C3E) workshop. C3E brings together participants from government, industry, and academia to learn about and propose solutions to problems related to cyberspace. A prominent feature of the C3E workshop is a real-world challenge problem. Participating groups use sanitized data to generate solutions. Leveraging DNS logs containing 7.7 billion raw records, the ETC team proposed techniques for detecting and identifying malicious and potentially infected hosts.

Going forward, the ETC will conduct studies and analysis for SCORE. It will also generate a vision for areas of interest SCORE is considering as part of its task to recommend cyber research priorities to the president. The ETC is uniquely suited for this work—its mission is to identify, demonstrate, extend, and apply emerging software technologies to meet critical government mission needs, and in executing that mission it can draw on the SEI's deep expertise in software engineering and cybersecurity.

"We bridge the gap to the outside world. We bring in the best ideas from everywhere," said ETC Director Matt Gaston.



U.S. Army's Telemedicine and Advanced Technology Research Center Pilots LEAP4BD to Evaluate Big Data Systems

Ian Gorton

John Klein

"Software is about making decisions in a space where all the requirements are never truly known."

—Ian Gorton

The U.S. Army Medical Research and Materiel Command's Telemedicine and Advanced Technology Research Center (TATRC) is supporting development of the Integrated Electronic Healthcare Record (iEHR). To make design decisions, architects needed data about how different NoSQL databases fit the iEHR system's requirements. To meet the challenge of selecting databases for big data systems, the SEI's Ian Gorton and John Klein developed the Lightweight Evaluation and Architecture Prototyping for Big Data method, or LEAP4BD. LEAP4BD is a systematic approach for selecting NoSQL technology to satisfy a system's requirements at an acceptable cost. Key benefits include feature evaluation criteria for NoSQL databases, which significantly speed up the analysis process, and a knowledge base that continues to grow as it stores the results of each new NoSQL evaluation.

Gorton and Klein worked with developers at TATRC to perform the evaluation. They deployed three NoSQL products in the SEI's Virtual Private Cloud—in several configurations that made different tradeoffs among performance, availability, and consistency—and executed tests with workloads that represented use cases of interest for the iEHR. Gorton says that "software is about making decisions in a space where all the requirements are never truly known." In this environment, Klein emphasizes "the importance of having a trusted knowledge base to support your decisions about which NoSQL database is best suited for your big data system." The LEAP4BD pilot provided TATRC with qualitative and quantitative analysis of the best NoSQL options for the new iEHR.

For more information about LEAP4BD and the SEI's research on big data, visit http://blog.sei.cmu.edu/archives.cfm/category/big-data**.**

CERT Data Study Highlights Utility of Analysis Approach

Angela Horneman

Deana Shick

The data fusion method Horneman and Shick documented can be used to explore an organization's IP space, which can be eye opening.

The Pudong district of Shanghai, China
Photo: Wechselberger

Two SEI researchers wondered if valuable cyber threat information could be culled from publicly available datasets to corroborate or contradict findings in the Advanced Persistent Threat 1 (APT1) report published by information security firm Mandiant. In its report, Mandiant characterized APT1 as the most prolific of the advanced threat actors it has studied, and it offered evidence that, according to Mandiant, demonstrated the espionage unit was operating out of the Pudong district of Shanghai, China. Angela Horneman and Deana Shick, both members of the technical staff in the SEI's CERT Division, analyzed a great deal of data and documented a method to provide insight into other areas of threat analysis.

Using publicly available information about APT1, Shick and Horneman did corroborate the Mandiant report, but the true value of their task was illustrating how much information about network assets is available when performing data fusion.

Shick and Horneman found that by combining certain data sets they could obtain much more information than other researchers previously had. Horneman and Shick detailed their method in the SEI Technical Report Investigating Advanced Persistent Threat 1 (APT1). Any researcher with time and something to investigate can uncover interesting data using the method described in the report.

Besides investigating known or suspected threat infrastructure to validate or identify threat indicators, the data fusion method Horneman and Shick documented can be used to explore an organization's IP space, which can be eye opening, and it could also indicate areas where security needs updating or complete rethinking.

Horneman and Shick plan to examine other sources of data using their analysis technique. They believe the technique offers a promising way to extract significant intelligence for many existing cybersecurity threats.

To learn more about this research, read the SEI report *Investigating Advanced Persistent Threat 1 (APT1)* at http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=90426.

New CERT Insider Threat Course Helps Organizations Meet Government Standards

Randy Trzeciak

"The Insider Threat Center is providing this training to help organizations develop an insider threat program that meets the requirements set forth in the Executive Order [13587]."

—Randy Trzeciak

In October 2011, President Obama signed Executive Order 13587, *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*. This order requires federal agencies that operate or access classified computer networks to implement insider threat detection and prevention programs. In addition, proposed changes to the National Industrial Security Program Operating Manual (NISPOM) would require the same of contractors that engage with such federal agencies.

To help organizations meet these requirements, the CERT Insider Threat Center launched the Insider Threat Program Manager (ITPM) Certificate. This CERT-developed training will help program managers charged with developing formal insider threat programs.

The training covers

- insider threat program planning
- identification of internal and external stakeholders
- components of insider threat programs
- insider threat team development and communication strategies
- program implementation

To complement this training, the CERT Insider Threat Center is also developing certificate programs on insider threat vulnerability assessments and insider threat program evaluations.

"The Insider Threat Center is providing this training to help organizations develop an insider threat program that meets the requirements set forth in the executive order," said Randy Trzeciak, technical manager of the Enterprise Threat and Vulnerability Management Team in the SEI's CERT Division. "We feel that by combining a technical and behavioral approach to addressing insider threat, organizations can create a program that mitigates the threat while at the same time protecting the privacy and civil liberties of employees."

For more information about the ITPM Certificate, visit http://www.cert.org/insiderthreat.

Secure Coding Team Continues Crusade for Safe Code

Software developers produce more than 1 billion lines of code every year of unknown quality. The 1.3 million significant lines of code (sigLOC) in Java analyzed by the CERT Source Code Analysis Laboratory (SCALe) averaged 39 secure coding violations per 1,000 sigLOC. The 9.7 million sigLOC of C and C++ code analyzed using SCALe fared even worse, with 76 violations per 1,000 sigLOC. Considering our critical reliance on software, code quality and security is a serious concern.

"Secure coding is extremely difficult, and programmers get less help than they should from their compilers and tools," said Robert C. Seacord, technical manager of the CERT Secure Coding Initiative. "Developers are frequently under pressure to deliver on schedule. Code quality and security may suffer as a result."

In 2014, Seacord's team created new tools to help developers avoid introducing vulnerabilities. These tools include the Clang Thread Safety Analysis (Clang TSA), which helps developers improve the security of code running in multi-core processing environments; DidFail and Mobile SCALe, which can help Android app developers prevent activity hijacking and data leaks; and new rules for secure C coding (see page 25).

Google Collaboration Nets Clang Thread Safety Analysis

The broad adoption of multi-core processors has made concurrency increasingly important. C and C++ languages have evolved to support multiple threads of execution, including improved memory models, and atomic objects and operations. These advances, however, have introduced the possibility of concurrency vulnerabilities when programming in these languages.

Working with DeLesley Hutchins of Google, the SEI's Aaron Ballman tackled the problem of thread safety analysis in multi-core environments. The collaboration resulted in the Clang TSA. This tool uses source code annotations to declare and enforce thread safety policies in C and C++ programs. The tool is part of Clang, a production-quality C and C++ compiler. Clang TSA is currently deployed on a large scale at Google, where it has gained widespread adoption. "Google had already developed thread safety analysis based on locks [synchronization mechanisms for enforcing limits on access to a resource in a multi-thread environment]," said Ballman. "The primary difference between our thread role-based approach and Google's lies in the terminology programmers use to annotate their programs. We decided to unify the two approaches. Google had already mandated that all programmers use lock-based analysis on all C++ code run within the company. Consequently, most of the underlying analysis was already vetted at scale in a production environment."

DidFail and Mobile SCALe Offer Help for Better Android Code

The Android operating system (OS) dominates the smartphone market. Unfortunately, applications developed for the Android OS have contained vulnerabilities that expose users to attacks such as activity hijacking, which occurs when a malicious app receives a message intended (but not explicitly designated) for another app. The attack can cause data leaks or the loss of control over targeted apps. SEI researchers Will Klieber and Lori Flynn created a static analyzer to detect likely activity-hijacking vulnerabilities in apps.

Another problem plaguing the Android OS is the prevalence of apps that leak private information. To help combat this problem, Klieber and Flynn created a taint flow analyzer called Droid Intent Data Flow Analysis for Information Leakage (DidFail) that combines and extends analyses of inter-component and intra-component dataflow in Android applications to analyze data flows within entire Android app sets. The long-term vision is for app stores to use DidFail to compute which data flows would be enabled by a new app before the user installs it, inform the user about these flows, and provide the user a mechanism for blocking undesired flows.

For more about Clang TSA, visit http://www.cert.org/secure-coding/tools/clang-thread-safety-analysis.cfm.

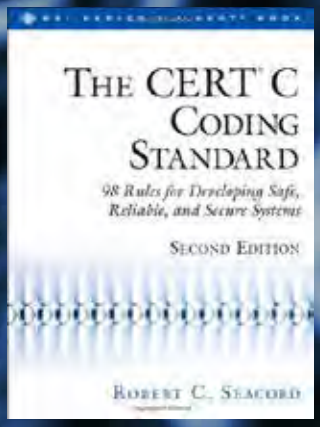
To learn more about DidFail, visit http://www.cert.org/secure-coding/tools/didfail.cfm.


Robert Seacord


Aaron Ballman


Lori Flynn


Will Klieber



Updated Standard Offers More Help with Secure C Coding

As part of its ongoing mission to help developers avoid coding errors and produce safe, reliable, and secure systems, the SEI's Secure Coding Team updated its C language coding standard in 2014. Published by Addison-Wesley Professional, The CERT C Coding Standard, Second Edition: 98 Rules for Developing Safe, Reliable, and Secure Systems has been greatly improved and incorporates contributions from numerous experts.

The CERT C Coding Standard, Second Edition, enumerates the coding errors that are the root causes of current software vulnerabilities in C, prioritizing them by severity, likelihood of exploitation, and remediation costs. "Secure programming in C can be more difficult than even many experienced programmers realize," said author Robert C. Seacord. "Software systems are becoming increasingly complex, even as our dependency on these systems increases. In our new CERT standard, as with all of our standards, we identify insecure coding practices and present secure alternatives that software developers can implement to reduce or eliminate vulnerabilities before deployment."

This new edition provides secure coding rules for the new C11 standard, including a new chapter on concurrency. The rules can also be applied to earlier editions of the C language, such as C99.

To learn more about this publication, visit http://www.cert.org/secure-coding/publications/books/cert-c-coding-standard-second-edition.cfm.

SEI Expands the Utility of the Smart Grid Maturity Model

Julia Mullaney

"These virtual navigations are another way for us to make the SGMM accessible even to smaller utilities with limited resources. The eight utilities who piloted this approach really liked the staggered sessions."
—Julia Mullaney

Virtual Course Broadens Access to Navigator Training
Making the Smart Grid Maturity Model (SGMM) more useful for utility companies—that was the challenge a number of SEI researchers took on in 2014. Their first step was to launch a virtual version of the SGMM Navigator Training course. The course teaches potential SGMM Navigators how to use the SGMM Navigation process to help utilities assess the state of their grid modernization programs. Navigation helps utilities understand their current status, set aspirations, and measure progress toward those aspirations. Students can now participate in live lectures by skilled SEI instructors, ask questions in real time, and learn as a team without having to travel for on-site instruction.

Pilot Addresses Smaller Utilities
The SEI also piloted Virtual Navigations, an innovative way to make the Navigation process accessible to smaller utilities. The SEI partnered with the American Public Power Association (APPA) and Leidos (formerly Science Applications International Corporation [SAIC]) to develop Virtual Navigations. In the pilot, SEI-Certified Navigator Steve Rupp of Leidos led a group of eight public power utilities through six short sessions spread out over six weeks. Assessment and aspiration setting took place in two-hour blocks. According to Julia Mullaney, manager of the SGMM project, "These virtual navigations are another way for us to make the SGMM accessible even to smaller utilities with limited resources. The eight utilities who piloted this approach really liked the staggered sessions."

The SGMM project currently has 15 industry partners and 36 certified and candidate SGMM Navigators.

For more information about SGMM, visit http://www.sei.cmu.edu/smartgrid/index.cfm.

SEI's Software Assurance Competency Model Earns IEEE Endorsement

Nancy Mead

"IEEE endorsement helps to maximize our outreach and impact. In addition, the SwA Competency Model was mapped to the newly developed DHS competencies, thereby also supporting one of our major sponsors."
—Nancy Mead

In 2013, the SEI published the Software Assurance (SwA) Competency Model, developed to help organizations and individuals determine SwA competency across a range of knowledge areas and units. The model provides a capability for an organization to adapt the model's framework to the organization's particular domain, culture, employee position descriptions, or structure.

Since its release, the model has been used to provide the U.S. Department of Homeland Security (DHS) and other employers of SwA personnel with a means to assess the SwA capabilities of current and potential employees, and to build teams with the needed mix of SwA skills. The model has also served to

- offer guidance to academic or training organizations that develop SwA courses to support the needs of organizations that are hiring and developing SwA professionals
- enhance SwA curricula guidance by providing information about industry needs and expectations for competent SwA professionals
- provide direction and a progression for the development and career planning of SwA professionals
- provide support for professional certification and licensing activities

In 2014, the Software and Systems Engineering Committee of the IEEE Computer Society Professional Activities Board (PAB) endorsed the SEI Software Assurance Competency Model as appropriate for software assurance roles and consistent with *A Framework for PAB Competency Models*.

"In our SwA competency and curriculum work, it has always been our goal to be consistent with IEEE guidelines and to request IEEE endorsement," said Nancy Mead, SEI fellow and principle researcher. "IEEE endorsement helps to maximize our outreach and impact. In addition, the SwA Competency Model was mapped to the newly developed DHS competencies, thereby also supporting one of our major sponsors."

For more information about SWA Competency Model, visit http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=47953.

Vulnerability Assessments Help Federal Agencies Understand Their Specific Risks


Brent Kennedy

"Conducting assessments that implement realistic threat emulation and aggressive attacks is one of the best things an organization can do to truly understand the vulnerabilities and inherent risk within its infrastructure."

—Brent Kennedy

Over the past three years, the SEI's CERT Division has helped federal agencies gain insight into their susceptibility to catastrophic cybersecurity breaches by conducting Risk and Vulnerability Assessments (RVAs). Through data gathering and rigorous testing, the CERT Division's Cybersecurity Assurance Team has identified cybersecurity risks within these organizations and aided in their mitigation. Until recently, the CERT Division conducted RVAs exclusively for federal government agencies. In 2014, the team began to perform these assessments for state and local governments, as well as private industry owners and operators of critical infrastructure.

The knowledge the team has gained through its work for the Department of Homeland Security (DHS) National Cybersecurity Assessment and Technical Services helps seed innovative research and advance the state of the practice. In 2014, the SEI collaborated with DHS to conduct more than 39 RVAs. This unique opportunity enabled the SEI to make an immediate and direct impact on current cybersecurity issues, such as the Heartbleed vulnerability. This vulnerability was a flaw in the OpenSSL cryptography library that affected thousands of hosts across the internet and could potentially result in data leakage. The RVA assessments conducted with DHS provided a unique opportunity to view the security posture of small and large government organizations alike and secure assets of national importance, such as the healthcare.gov platform.

During an RVA, the CERT team combines national-level threat and vulnerability information with data collected and discovered on the networks of the participating organization. This information enables the team to provide tailored risk analysis reports and actionable remediation recommendations prioritized by risk level. These services complement an organization's existing security program and capabilities and provide an objective view of its security posture.

The RVA engagements offer full-scope red team/penetration testing capabilities and methodologies that are constantly being refined and updated with new techniques and more efficient processes. According to Brent Kennedy, the SEI project lead, "Conducting assessments that implement realistic threat emulation and aggressive attacks is one of the best things an organization can do to truly understand the vulnerabilities and inherent risk within its infrastructure. Scheduling these assessments on a periodic basis allows for organizations to adapt to new and changing threats and provide insight into the strengths of their external and internal defenses."

RVA services and capabilities are multi-faceted. They include

- vulnerability scanning and testing: using manual and automated methods to identify software vulnerabilities
- penetration testing: exploiting weaknesses and attempting to gain further control of the target network
- social engineering (phishing): sending a crafted email to a targeted audience to test security awareness
- wireless discovery and identification: identifying wireless signals (including identification of rogue wireless devices) and exploiting access points and guest networks
- web application scanning and testing: identifying vulnerabilities and weaknesses specific to web applications
- database scanning: conducting a security scan of database settings and controls
- operating system scanning: conducting a security scan of the organization's operating system to achieve compliance checks

As the program continues to grow and serve more critical infrastructure organizations, the CERT team plans to analyze data to provide unique, sector-focused insights. This analysis supports custom assessments to give organizations increasingly accurate pictures of their specific threats and cybersecurity challenges.

Where the Money Goes: Understanding Sustainment Funding Decisions

Photo courtesy of U.S. Navy.

Andrew Moore, Sarah Sheard, Bob Ferguson, Mike Phillips

"NAVAIR found that our model, calibrated with their data, could accurately respond in a way that mirrored their real-world experiences."

—Bob Ferguson

The word *sustainment* can mean a lot of things in the Department of Defense (DoD). Sustaining hardware may involve removing corrosion or replacing worn parts. If a part is no longer available, or if its performance requires improvement, hardware sustainment may expand to include design and engineering. Sustaining software-intensive products substantially changes the mix of work performed. "Software design changes are commonplace, and even writing large amounts of new code can fall under the 'sustainment' phase of the lifecycle," said Bob Ferguson, senior member of the SEI technical staff. "This means the rules are changing for deciding how much money is needed for sustainment and where those funds should be spent."

To facilitate sustainment decision making, the SEI developed a dynamic model that can show those responsible for funding decisions how budgeting, resource allocation, mission performance, and strategic planning are interrelated. "A decision made by one stakeholder can affect the performance of many others," said SEI senior engineer Sarah Sheard. "The model shows how delaying a decision to fund an improvement, for example, can reduce the ability of a sustainment organization to provide warfighter capability."

To determine whether the model would work in the real world, the SEI collaborated with Naval Air Systems Command (NAVAIR) personnel at the Advanced Weapons Lab at China Lake, Calif. "NAVAIR found that our model, calibrated with their data, could accurately respond in a way that mirrored their real-world experiences," said Ferguson. "This led them to adopt the model as a way to help program leaders make more informed decisions about resource allocation in light of the potential impacts those decisions may have on all stakeholders in the sustainment ecosystem."

For more on the SEI's research on sustainment models, visit http://www.sei.cmu.edu/measurement/research/sustainment-investment/index.cfm**.**

SEI Teams Collaborate to Tackle Defense Intelligence Framework Challenges

In an era of belt tightening, the federal government is looking to move away from stove-piped software development toward open, reusable architectures. It wants to employ these reusable architectures to leverage existing technology, curtail wasted effort, and add capabilities. For example, the Department of Defense (DoD) is concentrating on the development of service-oriented architectures and common technical frameworks for the Defense Intelligence Information Enterprise (DI2E). To help the government navigate challenges related to the DI2E Framework (DI2E-F), which promotes reuse in building defense intelligence systems, a cross-functional team of SEI researchers was tapped in 2014 to lend its expertise.

The team, which comprises researchers from the SEI's Emerging Technology Center (ETC) and the CERT Division's Secure Coding Initiative, focused on supporting development of the DI2E-F. "The framework provides the Defense Intelligence Community the building blocks needed to more efficiently, effectively, and securely develop, deliver, and interface mission architectures," said Derrick H. Karimi, software developer in the ETC and the SEI's lead on this project. "Its core components satisfy standards and specifications, including web service specifications, that enable a stable, agile enterprise that supports rapid technology insertion."

When completed, the DI2E will provide a fully integrated, cross-domain, globally connected, all-source intelligence enterprise that comprises the federated intelligence mission architectures of the military services: combat support agencies, combatant commands, the intelligence community, and international partners.

The DI2E-F will provide a storefront for software that

- transforms information collected for intelligence needs into forms suitable for further analysis and action
- provides the ability to integrate, evaluate, interpret, and predict current and future operations or physical environments
- provides the ability to present, distribute, or make available intelligence, information, environmental content, and products that provide better situational awareness to military and national decision makers

The SEI's work on this project, which was undertaken by Michelle Barker, Ryan Casey, Karimi, Daniel Plakosh, Robert Seacord, David Shepard, David Svoboda, and Eric Werner, spans two fronts:

1. helping the DoD develop the framework by providing feedback to the DI2E-F Program Management Office about framework processes and practices
2. evaluating specific components to be included in the software reuse initiative

As part of its open-architecture approach, the government intends to take advantage of free and open source software, government off-the-shelf software, and commercial off-the-shelf software. Also, when necessary, it will develop new software that satisfies any identified gaps needed to complete the DI2E enterprise. In support of this effort, the SEI team contributed to the design of the software component evaluation and the development of software tools created to automate evaluation tasks. It also performed the software evaluations necessary to ensure quality reusable components are recommended for reuse.

Derrick H. Karimi

"The [DI2E] framework provides the Defense Intelligence Community the building blocks needed to more efficiently, effectively, and securely develop, deliver, and interface mission architectures."

—Derrick H. Karimi

The SEI team also conducted software component evaluations that align with the ETC's areas of expertise in data-intensive scalable computing. "These evaluations focused not only on reusability, but also on security, including code analysis," said Karimi. "The code work was directed by researchers in the CERT Secure Coding Initiative, who maintain a laboratory environment for static analysis." The Source Code Analysis Laboratory (SCALe) employs commercial, open source, and experimental tools to analyze various code bases.

The SEI's work on DI2E-F aligns with the ETC's mission, which is to promote government awareness and knowledge of emerging technologies and their application and to shape and leverage academic and industrial research. This work also demonstrates how teams from across the SEI's multiple divisions can collaborate in support of sponsors' needs and objectives.

For more on the SEI's work in support of DI2E, visit http://blog.sei.cmu.edu/post.cfm/open-architectures-defense-intelligence-300.

SEI STEM Initiative Gives Kids Sweet Challenge at USA Science & Engineering Festival

Connie Sapienza

Bob Rosenstein

Jim McHale

"We had approximately 3,500 visitors to our booth. The kids loved it. Many adults said they were going to re-use our idea in their programs."

—Connie Sapienza

"How many candies are in that jar?" That's the question the "SEI Candy Factory" put to kids attending the 2014 USA Science & Engineering Festival in Washington, D.C. The four-day, biennial event, which last year drew 325,000 attendees, is designed to advance science, technology, engineering, and mathematics (STEM) education. The SEI was both an exhibitor and a sponsor of the event.

The idea behind the SEI's candy game was not to generate wild guesses, but to get kids thinking about the science of estimation. "The game was based on an exercise I developed for our Team Software Process℠ (TSP℠) Team Member Training," said the SEI's Jim McHale, a senior member of the technical staff, "but I didn't see any reason it wouldn't work for kids since we could coach them through the thought process." Estimation informs numerous tasks undertaken by the SEI for its clients.

For instance, the SEI uses sophisticated estimation techniques to determine how much code a planned system will require and the time and effort needed to create it.

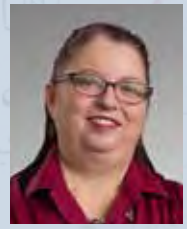
The SEI's exhibit was well received. "We had approximately 3,500 visitors to our booth," said Connie Sapienza, exhibit lead for the SEI. "The kids loved it. Many adults said they were going to reuse our idea in their programs."

Bob Rosenstein, SEI business manager, noted the festival was a unique way for the SEI to reach thousands of school-aged children. "It was fascinating to work with various age groups on the estimation game," said Rosenstein. "Some used pen and paper, others used their smartphones, but all were determined to get as close as possible to the correct answer. We interacted with many families, and a vast majority of the parents knew immediately who Carnegie Mellon University was. The feedback was very positive."

For more information about the USA Science & Engineering Festival, visit http://www.usasciencefestival.org/about.html.

Illustrating Agile for Better Understanding


Mary Ann Lapham


Suzanne Miller


Kurt Hess

The SEI's Agile Adoption in Government Settings project helps acquisition professionals in the Department of Defense (DoD) and other federal agencies interact effectively with contractors who use Agile methods. The biggest hurdles include new terminology, unfamiliar processes and procedures, and the need for a collaborative acquisition culture. So, in 2014, the SEI's Agile team undertook several projects to make Agile concepts more accessible.

"We pursued three approaches," said the SEI's Suzanne Miller, "and continued an effective working relationship with Kurt Hess, an illustrator in the SEI's Creative Communications team."

Hess first learned Agile concepts, then supported the Agile team by making "graphical recordings" during meetings of the Agile Collaboration Group. "Kurt transformed key points into hand-drawn murals that were amusing and relevant to difficult concepts," said Miller. "His images crystallized these concepts, and they are often requested by group members for their own use."

The SEI team also produced a tutorial called "Agile Mythbusting." First presented at the Ground Systems Architecture Workshop, the SEI delivered the tutorial (which employs Hess's illustrations) to help debunk myths about Agile use in government.

"The tutorial was so well received we created the booklet *Agile Development in Government: Myths, Monsters, and Fables*," said Miller. Hess illustrated the booklet, whose lead author is the SEI's David Carney. "The booklet presents a somewhat tongue-in-cheek reflection on certain attitudes toward Agile software development," said Miller. The myths addressed by the booklet include "Agile is a fad" and "Agile is cowboy programming."

"Our goal," said Miller, "was to cast light on inaccuracies and misunderstandings in a light-hearted manner."

For more on Agile research at the SEI, visit:
http://blog.sei.cmu.edu/archives.cfm/category/agile.

Big Ideas for Big Data: Hardware, Software, Analysis, and Teaching for Graph Analytics

As big data gets bigger and more complex, solutions for extracting meaning from that data—in particular, identifying patterns, relationships, and predictions—becomes an even bigger challenge. Graph analytics, a way of understanding relationships among people, locations, and items, is emerging as an incredibly powerful solution for extracting meaning from large datasets.

Researchers at the SEI's Emerging Technology Center (ETC) have been working on graph analytics since 2012. "Graph analytics research is a natural fit for us," said Eric Werner, technical director of the center, "because it aligns so well with our mission to bring new and emerging technologies to bear on government challenges."

Graph analytics are commonly used in social networks and web search, as well as to prevent fraud and analyze customer perceptions. Graph analytics can also be applied in fields such as cybersecurity, robotics, and knowledge discovery.

Researchers from the ETC are applying graph analytics to hardware, software, and analysis challenges, and they are teaching others what they learn. In January 2014, a team of researchers applied their knowledge of graph analytics to a challenge problem posed at the Computational Cybersecurity in Compromised Environments (C3E) workshop, sponsored by the Special Cyber Operations Research and Engineering (SCORE) Interagency Working Group. "Our task in the challenge problem was to look at a large set of anonymized data to identify advanced persistent threats," said Scott McMillan. "We used whitelists to reduce the billions of records provided, then we used graph analysis to identify anomalous patterns of connection activity within the remaining records," he added. The solution performed well.

Researchers from the ETC are also investigating emerging hardware architectures: current systems simply can't keep up with the complex operations required by graph analytics. "We are creating a software library that can exploit heterogeneous parallel computers—that is, computing systems with a variety of processing architectures, such as central processing units (CPUs) and graphics processing units (GPUs)—and enable developers to create systems that are more efficient in terms of computation and power consumption," said Werner. He added, "We hope our research will enable programmers in government and industry to use our software library to more easily create effective software for future computing systems." The team's next step is to release the library to stakeholders in the DoD and to other users as open source software.

To help develop knowledge and skills in this field for one of the SEI's government customers, researchers Scott McMillan and Stephanie Rosenthal created a four-day, hands-on training course in predictive analytics—a field closely related to graph analytics. "We designed the course so that participants could gain an advanced understanding of predictive analytics—including data mining, machine learning, natural language processing, and graph analytics—through hands-on experience with real-world problems," said Rosenthal. McMillan and Rosenthal worked with the customer to select and develop problem sets tailored for course participants. They plan to adapt the course for other organizations in the future.

"Graph analytics is becoming more important and more pervasive," said Werner, "and our work will help our customers better exploit this powerful technique."


Scott McMillan


Eric Werner


Stephanie Rosenthal

"We are creating a software library that can exploit heterogeneous parallel computers—that is, computing systems with a variety of processing architectures, such as central processing units and graphics processing units—and enable developers to create systems that are more efficient."

—Eric Werner

Empirical Research Office Fosters Data-Driven Approach to Acquisitions

At the Department of Defense (DoD)—an organization that thrives on data and relies on software-based systems—there is a lack of information in one very important area: software development and acquisition. As software plays an increasing role in critical warfighter capabilities and the DoD continues to increase its software investment, the need for such data only continues to grow.

To address this gap, the SEI created the Empirical Research Office (ERO). Under the leadership of Associate Director David Zubrow, Assistant Director Forrest Shull, and Software Solutions Deputy Director Anita Carleton, the ERO spearheads research to support policy and program-management decisions about software systems. Its work aligns with the priorities for data-driven decision making defined in the DoD Better Buying Power and the Air Force Bending the Cost Curve initiatives. The goal of the ERO is to become the DoD's go-to source for empirically grounded information in the areas of software acquisition, development, and sustainment.

"We're the only FFRDC focused on software engineering," said Shull. "This makes us uniquely suited to lead this work. Our goal is to provide decision makers credible and practical advice on policy related to the DoD's substantial investments in software systems, relying on measure-based evaluations of program health and emerging technologies."

The ERO is currently laying the foundation by diving into data from programs on cost, quality, and schedule progress. The work examines how data reported by contractors is analyzed and reported to convey program status, and is rolled up to characterize portfolio and enterprise characteristics and program performance.

"Analyzing data across multiple levels of granularity better positions ERO analysts to develop and validate leading indicators of program health," said Shull. "It also identifies best practices currently in use and gaps that need to be addressed." Shull noted that the ERO's approach enables analysts to understand the provenance, quality, and completeness of the data, ensuring that the limits of analyses are well understood.

From this foundation, Shull identified three research paths for the ERO. "First, we're undertaking data-driven analyses of DoD software acquisition programs to baseline current acquisition and development practice to ensure future research focuses on the right problems." For example, the ERO examined the average productivity of software development teams for various classes of systems and provided typical ranges for the different system types. "In the process, we're identifying the DoD's recurring software-related challenges," said Shull. The work is investigating questions such as

- What types of software development are most costly or uncertain?
- What is the difference between best-in-class and worst-in-class software projects?
- Which software technologies are problematic for software sustainment?

"The second research path will quantify the costs and benefits of various emerging solutions," noted Shull. Research topics in this path will take up questions such as

- How accurate and effective are virtual prototyping systems in providing early feedback on the cost effectiveness of new systems?
- How can the ROI of new software development paradigms, like model-based engineering, be calculated?
- What measures of program technical debt can be extracted automatically from a software code base?

"Third, we want to create the infrastructure and tools needed to support low-cost analysis," said Shull. Work here might leverage the data to facilitate collaborations with other FFRDCs and the larger research community. "Given the size of the undertaking," said Shull, "community engagement is critical. We want to involve researchers and subject matter experts who can elevate the quality of the research and improve the overall capability of the effort," he said.

For more information about the SEI's Empirical Research Office, contact ssd-empirical-research@sei.cmu.edu.


David Zubrow


Forrest Shull


Anita Carleton

Transition

The SEI accelerates the impact of software and cybersecurity improvements by working to promote adoption of improved capabilities by the defense industrial base and the wider software and cybersecurity communities. The SEI does this by creating standards, prototypes and tools, technical guidance, and platforms for knowledge and skill acquisition.

Standards

The SEI develops standards that improve the software ecosystem on which the Department of Defense (DoD) relies. For instance, the CERT Secure Coding Initiative has been leading the community development of secure coding standards for common programming languages. Many of these proposed practices are in use by major participants in the supply chain for DoD software-reliant systems, including Cisco Systems and Oracle. The SEI has also worked to integrate several research technologies into the Architecture Analysis and Design Language standard, making it extensible and semantically well defined. Application of the standard promotes the virtual integration of system building and testing activities—an approach that supports DoD objectives of achieving integrated warfighting capabilities and delivering solutions sooner to warfighters.

Prototypes and Tools

SEI researchers develop software prototypes that test proposed solutions, like the smartphone app developed in collaboration with the Carnegie Mellon University Human-Computer Interaction Institute. Called the Edge Mission-Oriented Tactical App Generator (eMONTAGE), this software program for mobile devices enables warfighters to mash data from multiple sources and view the results on a unified display—all without writing code. SEI researchers have demonstrated an eMONTAGE prototype at the U.S. Special Operations Command/Naval Postgraduate School (NPS) Tactical Network Testbed and at NPS's Joint Interagency Field Exploration (JIFX).

Tools

The SEI systematically builds software tools, especially those that address acute cybersecurity needs. Fuzz-testers and debuggers developed by the SEI's CERT Division, for example, can position military software engineers to meet requirements outlined in the 2013 National Defense Authorization Act for software assurance testing. Other SEI tools facilitate security analysis in large networks, enable analysts to rapidly query large sets of data traffic volumes, process packet data into bidirectional flow records, and simplify the building of analysis environments.

Technical Guidance, Workforce Development, and Knowledge Sharing

The SEI shares the progress and results of its research through a host of media avenues, including

- technical reports, blog entries, webinars, and podcasts available on its websites
- articles in prestigious professional journals and in publications geared to practitioners
- books in the SEI Series in Software Engineering published by Addison-Wesley

Those books often form the basis for education materials and training courses offered by the SEI and others. The SEI offers classroom and eLearning courses in software acquisition, network security, insider threat, software architecture, software product lines, software management, and other areas.

In 2012, the SEI introduced the CERT STEPfwd (Simulation, Training, and Exercise Platform) to help cybersecurity practitioners and their teams continually build knowledge, skills, and experience.

In addition, SEI researchers collaborated with educators from around the United States to develop the first curriculum for software assurance, the Master of Software Assurance (MSwA). The IEEE Computer Society and Association for Computing Machinery, as well as community leaders in curriculum development, formally recognized the MSwA Reference Curriculum as suitable for creating graduate programs or tracks in software assurance.

Leadership

Carnegie Mellon University Leadership

Subra Suresh
President
Carnegie Mellon University

Farnam Jahanian
Provost
Carnegie Mellon University

SEI Executive Leadership Team

Seated: David Thompson, Chief Information Officer; Robert Behler, Deputy Director and Chief Operating Officer; Kevin Fall, Deputy Director and Chief Technology Officer; Mary Catherine Ward, Chief Strategy Officer

Standing: Matthew E. Gaston, Director, SEI Emerging Technology Center; Peter Menniti, Chief Financial Officer; Paul Nielsen, Director and Chief Executive Officer; Richard Pethia, Director, CERT Division; John Bramer, Chief of Staff; Edward Deets, Director, Software Solutions Division

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

Claude M. Bolton
Executive-in-Residence, Defense Acquisition University; former Assistant Secretary of the Army for Acquisition, Logistics, and Technology

William Bowes
Aerospace Consultant; Vice Admiral, USN (Ret.); former Commander, Naval Air Systems Command, and Principal Deputy Assistant Secretary of the Navy for Research, Development, and Acquisition

Christine Davis
Consultant; former Executive Vice President, Raytheon Systems Company

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

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

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

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

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

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

SEI Organizational Chart

SEI DIRECTOR'S OFFICE

Paul D. Nielsen
Director and Chief Executive Officer

Robert Behler
Deputy Director and Chief Operating Officer

Kevin Fall
Deputy Director and Chief Technology Officer

SOFTWARE SOLUTIONS DIVISION

Edward Deets
Director

Anita Carleton
Deputy Director

Linda Northrop
Chief Scientist

CERT DIVISION

Richard Pethia
Director

Bill Wilson
Deputy Director

Greg Shannon
Chief Scientist

EMERGING TECHNOLOGY CENTER

Matthew E. Gaston
Director

OFFICE OF CHIEF OF STAFF/ OFFICE OF CHIEF INFORMATION OFFICER

John Bramer
Chief of Staff

David Thompson
Chief of Staff

STRATEGIC INITIATIVES OFFICE

Mary Catherine Ward
Chief Strategy Officer

FINANCIAL AND BUSINESS SERVICES

Peter Menniti
Chief Financial Officer

SEI LEGAL

Sandra Brown
SEI General Counsel

SEI Staff And Other Contributors

As of September 30, 2014

Full-Time & Part-Time Employees

Lisa Abel
Steve Ader
Laura Aguera
Cecilia Albert
Christopher J. Alberts
Michael J. Albrethsen
William T. Aldrich-Thorpe
Dennis M. Allen
Julia H. Allen
Noelle K. Allon
Amanda Alvarez
Rogelio G. Alvillar
Laura Anderson
William B. Anderson
Bjorn Andersson
Eileen Angulo
John F. Antonucci
Luiz Antunes
Jeffrey J. Apolis
Melissa Argenziano
Leena Arora
Christopher A. Atwood
Felix H. Bachmann
Marie A. Baker
Karen A. Balistreri
Vincent F. Balistreri
Aaron Ballman
Jeffrey Balmert
Ronald M. Bandes
Michael Bandor
Michelle Barker
Hollen L. Barmer
Peter Barrett
Jeffrey J. Basista
Barbora Batokova
Roger A. Beard
Dwight S. Beaver
Stephen Ronald Beck
Robert F. Behler
Stephany Bellomo
Klaus Bellon
Jonathan F. Bender
Brian D. Benestelli
Kathleen E. Bennett
Anna M. Berta
Shawn D. Besselman
James Besterci
Robert Beveridge
Philip Bianco
David Biber
Daniel R. Bidwa
Darlene R. Bigos
Tracy A. Bills
Stephen Blanchette
Jeffrey L. Boleng
Elaine Bolster
Randall R. Bowser
Andrew D. Boyd
Diane I. Bradley
Ben W. Bradshaw
John R. Bramer
Kara Branby
Pamela A. Brandon
Heidi A. Brayer
Lea E. Bridi
Rex E. Brinker
Rita M. Briston
Rhonda M. Brown
Lisa L. Brownsword
Andrew M. Bunker
Matthew J. Butkovic
Palma Buttles-Valdez
Gene M. Cahill
Anthony F. Calabrese
Rachel L. Callison
Kimberley S. Campbell
Linda M. Campbell
Linda L. Canon
Peter S. Capell
Richard A. Caralli
Anita D. Carleton
Cassandra L. Carricato
Ryan M. Casey
William Casey
James J. Cebula
Anthony M. Cebzanov
Sagar J. Chaki
Mary Jo Chelosky
Timothy A. Chick
Leslie R. Chovan
Mary Beth Chrissis
Natalie Chronister
Jonathan C. Chu
Matthew T. Churilla
Jason W. Clark
Kathleen Clarke
William R. Claycomb
Matthew F. Coates
Cory F. Cohen
Julie B. Cohen
Sanford G. Cohen
Constantine Aaron Cois
Mary Lou Cole
Matthew Collins
James J. Conley
Anne M. Connell
Carol L. Connelly
James P. Conrad
Robert D. Conway
Stephen P. Cooney
Rebecca Cooper
Patricia A. Copelin
Stephanie L. Corbett
Alexander Corn
Daniel L. Costa
Jennifer Cowley
Randy Crawford
Rita C. Creel
Lucy M. Crocker
Larry J. Crowe
Stephanie D. Crowe
Michael E. Crowley
Natalie A. Cruz
Sally Cunningham
Pamela Curtis
Tenai J. Cutting
Jerome Czerwinski
Rebecca A. D'Acunto
Roman Danyliw
Rosemary J. Darr
Jeffrey H. Davenport
John Dayton
Dionisio De Niz
Edward H. Deets
Grant W. Deffenbaugh
Julien Delange
Nathan L. Dell
Kareem Demian
Matthew J. Desantis
Edward Desautels
Aaron M. Detwiler
Jill Diorio
John V. Diricco
Robert M. Ditmore
Mary C. Dixon
Geoffrey Dobson
Quintin A. Doles
George D. Doney
Patrick J. Donohoe
William A. Dormann
Audrey J. Dorofee
Joan P. Downing
Margie A. Drazba
Elke A. Drennan
Michael W. Duggan
Catherine A. Duncan
Evelyn Duncan
Madelaine Dusseau
Ladonna R. Dutton
Karin C. Dwyer
Sean D. Easton
James R. Edmondson
Danielle L. Edwards
Eileen A. Eicheldinger
Robin N. Eisenhart
Joseph P. Elm
Linda M. Elmer
Harold Ennulat
Lover E. Epps
Neil A. Ernst
Alan T. Evans
Felicia Evans
Sidney L. Faber
Michele E. Falce
Kevin R. Fall
Kimberly Farrah
Mariane Fazekas
Jeffrey Federoff
Peter H. Feiler
Eric Ferguson
Robert W. Ferguson
Donald G. Firesmith
Kodiak Firesmith
William L. Fithen
Robert W. Floodeen
Lori Flynn
Justin W. Forbes
John T. Foreman
Kunta Fossett
Arne Fostvedt
Summer Fowler
Tracey E. Fox
Jonathan J. Frederick
David C. French
Michelle C. Fried
Richard I. Friedberg
Jennifer R. Fritsch
Michael R. Fritz
Brent R. Frye
Michael J. Gagliardi
Douglas D. Gardner
Matthew Gaston
Linda P. Gates
Jeffrey Gennari
Lisa M. Gillenwater
Ryan Michael Gindhart
Ian Gorton
Walter J. Goss
Bruce A. Grant
Douglas A. Gray
Michael D. Greenwood
Phillip A. Groce
Charlene C. Gross
Jon L. Gross
Jacqueline Grubbs
Rajasekhar Gudapati
Arie Gurfinkel
Rotem Guttman
David A. Guzik
Shannon R. Haas
Barton L. Hackemack
Nancy L. Hags
John T. Haller
William R. Halpin
Jeffrey Hamed
Joshua A. Hammerstein
Charles B. Hammons
Michael Hanley
Jeffery Hansen
Stephen D. Hardesty
Erin Harper
Jeffrey S. Havrilla
Jason K. Hawk
William S. Hayes
Matthew Heckathorn
Jessica L. Hedges
Stephanie Hedges
Sharon Henley
Christopher Herr
Kurt Hess
Charles K. Hines
Scott A. Hissam
Barbara J. Hoerr
Bryon J. Holdt
Charles Holland
Andrew Hoover
Angela Horneman
Daniel P. Horvath
Allen Householder
Joshua R. Howell
John W. Huber
John J. Hudak
Clifford C. Huff
Lyndsi Hughes
Jennifer L. Hykes
Christopher Inacio
James Ivers
Jerry D. Jackson
Vanessa B. Jackson
Michael B. Jacobs
Michael Jehn
Zachary R. Jensen
John Connelly
John Hawrylak
George M. Jones
Jacob M. Joseph
Patricia Junker
Gavin T. Jurecko
Matthew H. Kaar
Stephen Kalinowski
Derrick H. Karimi
Rachel A. Kartch
Mark D. Kasunic
Harry P. Kaye
David Keaton
Tracey A. Kelly
Alexander Kem
Robert C. Kemerer
Brent Kennedy
Jennifer Kent
Carolyn M. Kernan
Christopher King
Kimberly King-Cortazzo
John R. Klein
Mark H. Klein
Stacy L. Klein
Mark Klepach
William E. Klieber
Dan J. Klinedinst
Georgeann L. Knorr
Andrew J. Kompanek
Michael D. Konrad
Keith Korzec
John J. Kostuch
Paul Krystosek
Robert E. Kubiak
Amy L. Kunkle
David S. Kyle
Michael L. Lambert
Joel Land
Debra J. Lange
Mary A. Lapham
Frank Latino
Alyssa Le Sage
Bernadette Ledwich
Ryan D. Lehman
Harry L. Levinson
Todd B. Lewellen
Darrell C. Lewis
Grace A. Lewis
Alena M. Leybovich
Amy J. Leyland
Joshua B. Lindauer
Martin M. Lindner
Howard F. Lipson

Murray R. Little
Todd S. Loizes
Gregory Longo
Melissa Ludwick
Richard W. Lynch
Rudolph T. Maceyko
Vamsi Maddula
Jimmy Mahomes
Lisa M. Makowski
Arthur A. Manion
Jay Marchetti
Attilio A. Marini
Tamara Marshall-Keim
Theodore F. Marz
Laura L. Mashione
Michael D. Massa
Kelly B. Matrazzo
Joseph P. Matthews
Roxanne Matthews
Jeffrey A. Mattson
Christopher J. May
Joseph Mayes
John J. McAllister
Michael McCord
Jason D. McCormick
James McCurley
Patricia McDonald
Shane P. McGraw
James D. McHale
David McIntire
Donna M. McIntyre
Janis M. McKinney
Bernadette McLaughlin
Michael McLendon
Joseph A. McLeod
Scott McMillan
Jason R. McNatt
Deborah S. McPherson
Nancy R. Mead
Ryan W. Meeuf
Nader Mehravari
Andrew O. Mellinger
Peter J. Menniti
Thomas J. Merendino
Jennifer C. Mersich
Leigh B. Metcalf
Bryce L. Meyer
Toby J. Meyer
Bertram C. Meyers
Amy Miller
Cassandra S. Miller
Gerald Miller
Suzanne M. Miller
Eugene E. Miluk
Marion V. Moeser
Soumyo Moitra
Elizabeth A. Monaco
Juan Maniquis Montelibano
Austin P. Montgomery
Andrew P. Moore
Jose Morales
Damon Morda
Gabriel A. Moreno
John F. Morley
Edwin J. Morris
Timothy B. Morrow
Anna Mosesso
Angela L. Mosqueda
Robert S. Murawski
David Murphy
Michael P. Murray
Paul J. Murray
Mark Musolino
Melissa S. Neely
Cynthia L. Nesta
Gail L. Newton
John O. Nicholas
William R. Nichols
Paul D. Nielsen
Crisanne C. Nolan
Robert Nord
Mika North
Linda M. Northrop
William E. Novak
Marc R. Novakouski
Kevin Nowicki
Jasmine Oates
Matthew O'Hanlon
Sharon R. Oliver
James W. Over
Ipek Ozkaya
Mariann Palestra
Timothy Palko
Steven Palmquist
Amanda Parente
Allison M. Parshall
Kevin G. Partridge
Nicole M. Pavetti
Carmal Payne
David J. Pekular
Kelwyn O. Pender
Brenda A. Penderville
Samuel Perl
Sharon K. Perry
Richard D. Pethia
Thomas Petrus
David M. Phillips
Dewanne M. Phillips
Janet R. Philpot
Patrick Place
Daniel Plakosh
Michael J. Pochan
Alicia N. Poling
William Pollak
Mary E. Popeck
Douglass E. Post
Jerome J. Pottmeyer
Katherine A. Prevost
Sean P. Provident
Kara M. Quinto
Traci M. Radzyniak
Angela Raible
James C. Ralston
Donald M. Ranta
Frank J. Redner
Aaron K. Reffett
Colleen A. Regan
David Reinoehl
Janet Rex
Clifford E. Rhoades
Louis A. Richards
Nathaniel J. Richmond
Michael A. Riley
Kimberly M. Ripple
John E. Robert
Lawrence R. Rogers
James D. Root
Steven W. Rosemergy
Robert Rosenstein
Sheila L. Rosenthal
Dominic A. Ross
Christian Roylo
Bradley P. Rubbo
Daniel J. Ruef
Robin M. Ruefle
Paul Ruggiero
Kristopher Rush
Russ Griffin
Mary Lou Russo
Mary Lynn Russo
Charles J. Ryan
Venkatavijaya Samanthapudi
Thomas M. Sammons
Charmaine C. Sample
Geoffrey T. Sanders
Concetta R. Sapienza
Emily E. Sarneso
Vijay S. Sarvepalli
Brian A. Satira
Jeffrey A. Savinda
Thomas P. Scanlon
Alfred R. Schenker
David A. Scherb
Robert B. Schiela
Andrew L. Schlackman
Steven Scholnick
Patricia L. Schreiber
James N. Schubert
Carol A. Schultz
Kenneth Schultz
Edward J. Schwartz
Giuseppe Sciulli
Tina Sciullo-Schade
Philip A. Scolieri
David Scott
Shirley M. Scott
William S. Scully
Johnathan R. Seaburn
Robert C. Seacord
Joseph Seibel
James S. Semler
Gregory E. Shannon
Sharon L. Shaw
Sarah A. Sheard
David J. Shepard
Mark S. Sherman
Nataliya Shevchenko
Deana M. Shick
Timothy J. Shimeall
Linda E. Shooer
Sandra L. Shrum
Forrest J. Shull
George J. Silowash
Soumya Simanta
Matthew P. Sisk
Lisa D. Sittler
Carol A. Sledge
Michelle A. Slusser
Holly L. Smith
James Smith
Lenny D. Smith
Timur D. Snoke
Tara R. Sparacino
Debra A. Spear
James Spencer
Derrick Spooner
Jonathan M. Spring
Bryan J. Springer
Bryan D. Stake
Lauren M. Stanko
Jonathan D. Steele
Katie J. Steiner
Lizann Stelmach
James F. Stevens
Katherine Stewart
Robert Stoddard
John P. Stogoski
Michael Stone
Edward R. Stoner
Jeremy R. Strozer
Gregory A. Such
Siobhan P. Sullivan
David Svoboda
Michael J. Szegedy
Lucille R. Tambellini
Joseph A. Tammariello
Christopher Taschner
Terry Ireland
Michael Theis
Marcia J. Theoret
Jeffrey Thieret
Kimberly E. Thiers
Alisa M. Thomas
Mark Thomas
William R. Thomas
David K. Thompson
Michele A. Tomasic
Barbara J. Tomchik
Carolyn Tomko
Brian M. Torbich
Troy Townsend
Helen L. Trautman
Peter J. Troxell
Donovan Truitt
Randall F. Trzeciak
Laurie A. Tyzenhaus
David E. Ulicne
Jeanette Urbanek
Vijay Sai Vadlamudi
Michelle A. Valdez
Christine Van Tol
Aaron M. Volkmann
Alexander Volynkin
Robert A. Vrtis
Todd O. Waits
Kurt C. Wallnau
Cynthia E. Walpole
Pennie B. Walters
Mary C. Ward
David A. Warren
Trina C. Washington
Andrea L. Wasick
Rhiannon L. Weaver
Michael Weber
Samuel M. Weber
Charles B. Weinstock
Eric B. Werner
James T. Wessel
Austin Whisnant
Barbara-Jane White
Amanda Wiehagen
Jeffrey A. Wiley
Pamela J. Williams
William R. Wilson
Craig J. Wink
Brian D. Wisniewski
Robert M. Wojcik
William G. Wood
Bronwyn Woods
Carol S. Woody
Lutz Wrage
Evan C. Wright
Michael A. Wright
Joseph Yankel
Charles G. Yarbrough
John W. Yarger
Hasan Yasar
Jamie L. Yoder
Lisa R. Young
Cat B. Zaccardi
Mark T. Zajicek
Marianne Zebrowski
John Zekany
Xiaobo Zhou
David Zubrow
Michael J. Zuccher

Other Contributors

Brian J. Averi
Donald R. Beynon
Tracy M. Cassidy
Peter Chen
Larry Druffel
Robert Ellison
Shane T. Ficorilli
Dennis R. Goldenson
John B. Goodenough
Frederick Kazman
Sung M. Lee
Julia L. Mullaney
Kenneth Nidiffer
Shauna Policicchio
Stephanie R. Pomerantz
Michael B. Rattigan
Douglas Schmidt
Lui Sha
Eileen O. Wrubel

Affiliates

Yoshiro Akiyama
Mary Lynn Penn
Martin Sebor
Yasutaka Shirai
Diego Vallespir

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM-0002345

The SEI Year in Review is produced by SEI Communication Services

Manager, Communication Services
William Thomas

Manager, Corporate & Technical Communications
Janet Rex

Manager, Public Relations
Richard Lynch

Editor-in-Chief
Ed Desautels

Editorial
Hollen Barmer
Heidi Brayer
Ed Desautels
Claire Dixon
Tamara L. Marshall-Keim
Gerald Miller
Nancy Ott
Sandra Shrum
Pennie Walters
Barbara White

Design
Cat Zaccardi

Illustration
Kurt Hess

Digital Production
Melissa Neely

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

Additional Information
Photo on page 13 courtesy of U.S. Marine Corps.
Typographical elements removed.

To determine how to put the SEI to work for your organization, contact SEI Customer Relations at info@sei.cmu.edu.

Work with the SEI

Congress established the SEI in 1984 because software is vital to the national interest. By working with the SEI, organizations benefit from more than two decades of government investment and participation from organizations worldwide in advancing the practice of software engineering.

The SEI creates, tests, refines, and disseminates a broad range of technologies, tools, and management techniques. These techniques enable organizations to improve the results of software projects, the quality and behavior of software systems, and the security and survivability of networked systems.

As an applied research and development center, the SEI brings immediate benefits to its research partners and long-term benefits to organizations that depend on software. The tools and methods developed by the SEI and its research partners are applied daily in organizations throughout the world.

How the SEI Works with Government and Industry

SEI staff members help the U.S. Department of Defense (DoD) and other government agencies solve software engineering and acquisition problems. SEI direct support is funded through task orders for government work. Engagements with the SEI are of particular benefit to government program managers, program executive officers, and senior acquisition executives, particularly those with long-range programs that will benefit from strategic improvements that the SEI fosters.

The SEI has a well-established process for contracting with government agencies and will work with an organization to meet its needs.

The SEI works with commercial organizations to develop a strategic advantage by rapidly applying improved software engineering technology.

The SEI works with organizations to combine their expertise with the SEI's expertise to mature new technology for the benefit of the entire software industry.

Customer Relations

Software Engineering Institute
Carnegie Mellon University
4500 Fifth Avenue
Pittsburgh, PA 15213-2612

1-888-201-4479 or 1-412-268-5800
info@sei.cmu.edu

SEI Employment

The SEI seeks candidates for its technical, business, and administrative divisions. To learn more about the benefits of working at the SEI, please visit www.sei.cmu.edu/careers.

Software Engineering Institute | Carnegie Mellon University

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

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

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