CONTENTS

MESSAGE FROM THE DIRECTOR 2

STRATEGY 3

AREAS OF WORK 3

OVERCOMING CHALLENGES IN THE FIELD WITH CLOUDLETS AND VIRTUAL MACHINES 4

DRIVING PRODUCTIVITY FOR THE F-22: THE BENEFIT OF SHOULD-COST ANALYSIS 7

INVESTIGATING THE VALUE OF AGILE IN ACQUISITION PROGRAMS 8

CECOM SOFTWARE ENGINEERING CENTER AMONG FIRST TO ADOPT THREE-MODEL CMMI APPROACH 9

USING MACHINE LEARNING TO DETECT MALWARE 10

ACCELERATED IMPROVEMENT METHOD (AIM) AT WORK IN THE AUTOMOTIVE INDUSTRY: THE SEI AND URBAN SCIENCE 12

MEETING THE CHALLENGE OF LARGE NETWORK MONITORING 14

CERT APPLIES SECURE CODING EXPERTISE TO NEW JAVA STANDARD 15

CERT ENHANCES THE USABILITY OF THE SMART GRID MATURITY MODEL WITH VERSION 1.2 15

BUILDING PUBLIC-PRIVATE PARTNERSHIPS IN CRITICAL INFRASTRUCTURE 16

PUTTING THE CERT RESILIENCE MANAGEMENT MODEL INTO PRACTICE 18

SEI ATTACKS MULTICORE CHALLENGES TO MISSION-CRITICAL DOD SYSTEMS 21

SEI TEAM JOINS NATIONAL SCIENCE FOUNDATION EFFORT ON EXTREME SCIENCE 22

SEI RESEARCH GROUP SEEKS MORE ACCURATE COST ESTIMATION 23

SEI EXPLORES METHODS TO IMPROVE DATA QUALITY THROUGH ANOMALY DETECTION AND NET SAVINGS FOR GOVERNMENT AND INDUSTRY 25

NORTHROP NAMED SEI FELLOW 26

MATT GASTON REFLECTS ON SEI INNOVATION CENTER ACCOMPLISHMENTS FOR 2011 27

ACQUISITION MODEL TO HELP PROGRAM OFFICES AVOID COMMON PITFALLS 29

CERT EXERCISE NETWORK (XNET) INSTRUMENTAL IN SUCCESSFUL EXERCISE IN CYBER ATTACK READINESS 30

TRANSITION 32

LEADERSHIP, MANAGEMENT, & STAFF 33

SEI DIRECTOR'S OFFICE 34

SEI MANAGEMENT 35

KEY PUBLICATIONS 36

STAFF AND OTHER CONTRIBUTORS 40
2011 was a record year for the SEI—a year of significant growth in our impact, in our influence, and in our initiative. Working with the Department of Defense (DoD), we sharpened the research focus of the Institute, added to our world-class staff, and received funding for the largest amount of new work the SEI has ever undertaken in one year. It was a year of leadership, excellence, and growth in software engineering.

The SEI’s success is really the success of its men and women. Across the Institute, the SEI is fortunate to have a skilled, smart, and inquisitive staff—some 600 people dedicated to excellence and innovation.

That dedication was recognized in 2011 at the individual level with the naming of Linda Northrop as an SEI fellow, a designation awarded to people who have made especially significant career contributions to the SEI and the software engineering community—and who continue to chart the future on key issues. Northrop, director of the Research, Technology, and System Solutions Program, is the Institute’s fifth SEI fellow. We congratulate her (see page 26).

2011 was also, unfortunately, a year of departures. We marked the retirement in September of Clyde Chittister, a 26-year SEI employee who served the organization as deputy director for operations and chief operating officer. And, shortly after the end of the fiscal year, Doug Schmidt—our deputy director for research and chief technology officer—announced his decision to return to Vanderbilt University to teach and mentor the next generation of researchers.

This report in many ways reflects the hard work and innovative thought of people such as Linda Northrop, Clyde Chittister, and Doug Schmidt, shared and amplified by our entire staff.

Among the many stories in these pages, here are glimpses of just a few:

- As the challenge to provide warfighters competitive advantage quickly has grown more acute, interest in Agile methods within the DoD acquisition community has also grown. In 2011, the SEI focused its investigation of Agile methods to develop guidance for DoD program managers, and plans to develop a companion contingency model in 2012 (see page 8).

- Two senior members of the technical staff at the SEI collaborated on a “should-cost” analysis of the software used in the F-22 modernization program. The Air Force program was one of the first to use the new should-cost estimation process (see page 7).

- Government and industry both want to know: “How can we improve, evaluate, and standardize the quality of data we use?” To begin to tackle this problem, SEI researchers collaborated with the Office of the Under Secretary of Defense (USD) for Acquisition, Technology, and Logistics (AT&L), Acquisition Visibility (AV). The team set out to evaluate statistical methods for improving on existing, manual methods of anomaly detection (see page 25).

- The Accelerated Improvement Method (AIM), streamlines CMMI adoption through a tailored version of the Team Software Process and Six Sigma measurement strategies. Helping organizations implement AIM is one way the SEI is increasing our focus on performance results (see page 12).

- The past year saw continued research by the SEI into addressing the challenges of monitoring large networks for malicious activity. The SEI’s approaches rely on techniques to summarize communications between hosts on the network. Even using summary techniques, monitoring large networks operated by the U.S. government and commercial enterprises generates huge volumes of data that security analysts cannot possibly analyze unassisted. Network Situational Awareness team members in the SEI’s CERT® Program have developed approaches to automate that analysis (see page 14).

Through these efforts and many more—and through the dedicated work of the entire SEI team—we are well positioned for the future. We’ll continue to enhance our research efforts while maintaining our excellent record of transition and acquisition support. I look forward to answering the challenges as we have done over the past quarter-century, and fully expect that the SEI will have a significant impact in 2012 and the years beyond.

Sincerely,

PAUL D. NIELSEN
Director and CEO
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 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 community 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.

AMPLIFY
The SEI works through the software engineering community and organizations dependent on software to encourage and support the widespread adoption of new and improved technologies and solutions through
• advocacy
• books and publications
• certifications
• 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 improvements.
The SEI engages directly with the community and through its partners to amplify its work.

AREAS OF WORK
The SEI technical program—created and carried out by world-recognized leaders in software engineering, security, and process management—consists of four technical programs. The SEI also conducts new research into emerging topics in software and systems engineering.

Quality software that is produced on schedule and within budget is a critical component to U.S. defense systems, which is why the U.S. Department of Defense (DoD) established the SEI in 1984. Since then, the SEI has advanced software and systems engineering principles and practices, while serving as a national and international resource for the software and systems engineering communities. As an applied research and development center, the SEI brings immediate benefits to its research partners and long-term benefits to the software industry as a whole.

Operated by Carnegie Mellon University—a global research university recognized worldwide for its world-class arts and technology programs—the SEI operates at the leading edge of technical innovation. The SEI’s core purpose is to help organizations improve their capabilities and to develop or acquire the right software, defect free, on time, and on budget, every time.

The SEI offers solutions to customers in the areas of
• Acquisition
• Process Management & Measurement
• Risk
• Security
• Software Development
• System Design

The SEI’s technical focus areas, together with its outreach activities, are aimed at meeting the defined software engineering needs of the DoD. Within these areas of work, the SEI collaborates with defense, government, industry, and academic institutions to continuously improve software-intensive systems. The SEI’s body of work in technical and management practices is focused on developing software right the first time, which results not only in higher quality, but also in predictable and improved schedule and cost.
A soldier on the ground learns that the enemy’s position has changed. On his handheld device, he revises the diagram depicting the battlefield configuration he has just sent his commander and sends her the new image. This time, however, the message isn't getting through—an enemy attack has cut off the connection. He quickly locates another connection through a nearby Humvee and successfully sends the image.

Handheld devices offer powerful potential in the battlefield. They can aid soldiers in tasks such as speech and image recognition, natural language processing, decision making, and mission planning. This is why researchers Grace Lewis, Soumya Simanta, and Dan Plakosh, members of the SEI Research, Technology, and System Solutions (RTSS) Program, are investigating ways to best leverage the full capabilities of handhelds. The SEI team is collaborating with Mahadev Satyanarayanan, creator of the cloudlet concept and a faculty member at Carnegie Mellon University’s School of Computer Science.

Their research addresses three main challenges. First, mobile devices offer less computational power than conventional desktops or server computers. Second, computation-intensive tasks, such as image or pattern recognition, take a heavy toll on battery power. Finally, networks have limited bandwidth and are unreliable.

“Our research explores ways to overcome these obstacles by using cloudlets, which are localized, lightweight servers running one or more virtual machines,” says Lewis. When soldiers must perform tasks that consume extensive memory or processing power, they can offload them to cloudlets from their handheld mobile devices to extend processing capacity and conserve battery.”

Cloudlets are located in physical proximity to the handheld devices that use them (for example, on Humvees). This reduces network latency because communication is limited to a single-hop network. Battery consumption potentially decreases through use of Wi-Fi instead of broadband wireless, which consumes more energy. From a security perspective, cloudlets can use Wi-Fi networks to take advantage of existing security policies that might prescribe, for example, certain encryption techniques or access only from specific handheld devices.

Additional advantages derive from use of virtual-machine (VM) technology. VM increases flexibility in the type and platform of applications and reduces software configuration and setup time. These properties are critical for systems used by soldiers or first responders working in dynamic and hostile environments where mission needs change rapidly and cyber resources are limited or subject to attacks. A form of VM technology called dynamic VM synthesis is particularly useful in such hostile environments. Its flexibility enables the use of opportunistically available resources, as well as rapid replacement of lost cyber resources.

Lewis summarizes her team’s future direction: “This year, in the first phase, we focused on creating a cloudlet prototype. In the second phase, we’ll conduct measurements to see if computations in a cloudlet provide significant reductions in device battery power. We’ll also gather measurements related to bandwidth consumption to focus on optimization of cloudlet setup time. Assuming we’re successful, we will use the third phase to create an experimental cloudlet cluster to explore other ways to take computation to the tactical edge.”
"Assuming we’re successful, we will use the third phase to create an experimental cloudlet cluster to explore other ways to take computation to the tactical edge.”

— GRACE LEWIS
“We aren’t just trying to sell a model or a method. We’re talking about doing things in a way that has proven to work, and if you don’t use the practices, you won’t get the performance.”

— Mike Phillips

1.7 MILLION

The F-22’s avionics software has 1.7 million lines of code.

PHOTO COURTESY OF USAF

ROBERT FERGUSON & MIKE PHILLIPS
DRIVING PRODUCTIVITY FOR THE F-22: THE BENEFIT OF SHOULD-COST ANALYSIS

“Do more without spending more,” urged Ashton Carter in a 2010 memo. Carter was then Under Secretary of Defense for Acquisition, Technology, and Logistics. His call for improved productivity advocated the use of should-cost estimates for major defense programs. Previously, program budgeting depended on estimates that forecasted what a project will cost based on past experience.

Carter called this “business-as-usual management” that essentially required programs to fully expend their budgets. Or, as the SEI’s Mike Phillips said, “Once you have that estimate, well, it never seems to come in any cheaper. With the next estimate based on the one preceding it, there is never an opportunity to account for the lessons learned that help software and systems developers get better at their work.”

Phillips and Robert Ferguson, both senior members of the technical staff at the SEI who work on the Software Engineering Measurement and Analysis initiative, collaborated on a should-cost analysis of the software used in the F-22 modernization program. The program, which includes upgrades to the aircraft’s air-to-ground and intelligence, surveillance, and reconnaissance capabilities, was one of the first Air Force programs to use the new should-cost estimation process.

“Our estimate succeeded in finding improvements that could significantly reduce the cost of the program,” said Ferguson. To calculate the should-cost estimate, the SEI used the data from the initial basis of the contractor’s estimate to create a parametric estimate that closely matched the contractor’s. The SEI then used the resulting model to test the sensitivity of the estimate and judge where potential savings could be found and how much could be saved. For example, team performance and estimates of quality could be compared to industry benchmarks. Contractors could then be encouraged to adopt improvements to improve development performance.

One significant source of savings came from improving quality at earlier stages of the lifecycle by adopting best practices. This reduced defects and lowered testing costs. As research has shown—including extensive data from the Team Software Process (TSP) work done at the SEI—repeated testing and defect-removal activities are very inefficient in terms of time and money. “Performance is correlated with using best practices early in the life cycle,” says Phillips. “We aren’t just trying to sell a model or a method. We’re talking about doing things in a way that has proven to work, and if you don’t use the practices, you won’t get the performance.”

The structure of the estimation models assumes that disciplined software development takes less effort than undisciplined development. “This is a reminder to organizations that there is value in bringing discipline to what they do. The estimation tool reflects that value. Estimators have an obligation to show managers the positive effects of high-process quality and high levels of development performance. Failure to improve performance could eventually make a contractor non-competitive,” Ferguson said.

Another interesting aspect of the F-22 program, according to Phillips, is the plan to focus first on software to increase capability. “People usually want to start with the hardware they want, and then develop software to support it,” he said. “Now they can get a lot of capability without having to do hardware upgrades to make it work.”

While updated hardware is also important to the F-22, rethinking development will enable the F-22 program to get capability improvements sooner. The package of upgrades that included hardware would only have demonstrated benefit in six years; by addressing software first, the estimated time was reduced to two and a half years.

Phillips, a former Air Force test pilot, thinks this shift in thinking is an interesting change. “Think of the way banks have changed,” he says. “There used to be lots of paper money going back and forth across the counter. Now the transactions are more and more electronic, and a bank is kind of like a big box with lots of ones and zeros in it. Now a supersonic jet can be thought of more and more as a bunch of ones and zeros with a plane around it.”

As the role of software in Department of Defense (DoD) programs has grown, the SEI has brokered compromise between contractors and DoD programs. Both parties must work to improve processes, and they must collaborate on compromises that save time and money without sacrificing quality. Should-cost estimation for software development makes an important contribution to the ultimate goal of making everything more affordable through a collaborative approach between industry and government.
“When applied properly in the right context, Agile can accelerate the delivery of high-value software capability.”
—Stephany Bellomo

AGILE:
An iterative and incremental (evolutionary) approach to software development. It is performed collaboratively by self-organizing teams within an effective governance framework. Our work in this area is led by Mary Ann Lapham.

INVESTIGATING THE VALUE OF AGILE IN ACQUISITION PROGRAMS

In 2008, then Secretary of Defense Robert Gates said, “Our conventional modernization programs seek a 99 percent solution in years. Stability and counterinsurgency missions—the wars we are in—require 75 percent solutions in months.” As the challenge to provide warfighters competitive advantage has grown more acute, interest in Agile methods within the Department of Defense (DoD) acquisition community has grown.

Agile is an iterative, incremental, and collaborative approach to software development. It features a lightweight, “just-enough” governance framework and is designed to be cost effective, timely, and adaptable. These qualities appeal to the DoD, which has a need for an acquisition tempo that responds to operational tempo, a need to obtain high-quality software within a dynamic environment, and a need to focus on value.

To support the DoD’s mission, the SEI’s Acquisition Support Program (ASP) has been investigating Agile methods. “When applied properly in the right context, Agile can accelerate the delivery of high-value software capability,” said Stephany Bellomo, chief engineer for civil and defense agencies in ASP. During the recently completed fiscal year, ASP conducted research on the successful use of Agile methods in the DoD and produced an evolutionary prototype for applying them. “Our research,” noted Bellomo, “is helping us develop guidance on the use of Agile in DoD acquisitions and the Agile Contingency Model, which will help the DoD determine when Agile might be a good fit for specific DoD projects.” By leveraging its ongoing relationships with DoD acquisition programs, the SEI is developing these resources to help the DoD make decisions about Agile methods that can help it achieve its goals for speed, adaptability, and efficiency.
CECOM SOFTWARE ENGINEERING CENTER AMONG FIRST TO ADOPT THREE-MODEL CMMI APPROACH

The U.S. Army Communications-Electronics Command (CECOM) Software Engineering Center (SEC) this year became one of the first organizations to adopt a process improvement strategy that employs all three CMMI models: CMMI for Acquisition, CMMI for Development, and CMMI for Services. The SEC’s mission is “to provide life-cycle software solutions and services that enable warfighting superiority and information dominance across the enterprise.”

“The SEC recognized that the work it performs extends beyond the focus of a single model for process improvement,” said Alex Stall, senior member of the technical staff at the SEI. “Building on the success of an SEC-wide Maturity Level 2 SCAMPI using CMMI for Development, it has identified areas in which it makes sense to use all three models to support process improvement across the organization.” Stall’s colleague Rusty Young, also a senior member of the technical staff, added that initial efforts have focused on identifying areas in which each model can be used exclusively to help the SEC meet process improvement and maturity-level objectives.

“SEC is a large, diverse organization that provides life-cycle software engineering capabilities that span the various phases of the Defense Acquisition Management Framework,” said Vickie Papa, chief, Strategic Transformation Division. “After achieving a CMMI-DEV Maturity Level 2 rating in 2010, we expanded our improvement initiative and created a model approach using the CMMI for ACQ/DEV/SVC to address the diversity of work within the SEC. We are implementing best practices of the models to improve our acquisition, development, and services processes across the SEC to gain process efficiencies while keeping a focus on customer needs, and to deliver timely, quality products and services to the soldier in the field.”
Malware, or malicious software, aims to disrupt operation, gather private information, and gain unauthorized access to system resources. SEI researcher Arie Gurfinkel noted that malware “spans the merely annoying to the financially dangerous to issues of national security.” Government and industry are increasingly concerned with malware, but much debate exists about the scope of the problem. Cory Cohen, a malware analyst with CERT, explained that experts’ counts range from 300,000 malware encounters per week to much higher numbers. Cohen’s SEI colleague Sagar Chaki pointed out, “The measurement problem is also a research problem.”
By a simple count, malware numbers are very high. But evidence indicates that most malware can be sorted into families of common origin. A few dozen families may account for the majority of detected malware instances. Chaki, who leads an SEI research effort to study malware detection, said that his team’s approach involved “getting a handle on the sheer number of malware encounters by finding similarities among them.”

“We have no ground truth in the malware domain,” added Cohen, so “classifying similarity in malware and understanding how many different kinds of malware exist will advance our understanding of the problem.”

Chaki, Cohen, and Gurﬁnkel are investigating executable software binaries that often take the form of malware. The variety and number of malware encounters make it difficult to construct a solution with a ﬁnite set of functions and mathematical operations. The team thought machine learning could provide a more effective solution. In machine learning, software can be “trained” on a set of known positive and negative examples.

The SEI team developed a method using a form of machine learning called classiﬁcation, which detects provenance similarities in binaries. These similarities indicate that the binaries were compiled from similar source code and with similar compilers. Using sample binaries to create a training set, the team trained a classiﬁer and then used it to predict the similarity of other binaries. Using machine learning, the team seeks to overcome the weaknesses of current labor-intensive manual techniques and of automated techniques that produce high false-positive or false-negative rates.

So far, the team has sampled open-source software because the ﬁeld lacks information about malware source codes and compilers. But the team thinks a classiﬁer that detects provenance similarity in open-source functions will also work with malware functions because variations between codes and compilers are largely independent of the software itself. While identifying similarities between binary functions remains a challenge, the team presented its preliminary results in a well-received paper at the 2011 Knowledge, Discovery, and Data Mining Conference in San Diego, California.

Eyeing future work, Gurﬁnkel explains there is still a scalability problem to solve: “The task needs to move from ‘given one thing, is another thing similar or not?’ to ‘given one thing, ﬁnd all things similar to it.’” Further research will explore other ways of detecting similarities between functions.
ACCELERATED IMPROVEMENT METHOD (AIM) AT WORK IN THE AUTOMOTIVE INDUSTRY: THE SEI AND URBAN SCIENCE

Gene Miluk, a senior member of the technical staff at the SEI, has been working with the consulting and software solutions firm Urban Science to help it enhance its process improvement capability. Miluk has extensive experience working with client organizations undertaking software process improvement, acquisition improvement, and technology transition. "Urban Science is working to develop a whole new generation of web-based tools to support its analytics technology," said Miluk. "This is a perfect example of a company searching for a better process technology and doing the necessary work to implement it. Their staff was great to work with, and they are now teaching their own people."

Urban Science, headquartered in Detroit, is a global company of automotive retail performance experts that provides advanced consulting and software solutions to help its clients increase market share and improve profitability. It has clients in more than 60 countries. The company uses scientific analysis and process-optimizing software to help automotive manufacturers better evaluate, structure, and manage their dealer networks and marketing programs. This year, with Miluk’s help, Urban Science adopted the Accelerated Improvement Method (AIM), a process improvement methodology developed at the SEI.

Process improvement is nothing new to Urban Science. For their new software development project, CIO Greg Davidson wanted a fast, effective approach. The company looked to AIM to provide a more structured approach to software development that would complement other methods used by Urban Science, such as Scrum. Using disciplined AIM processes starting with the Team Software Process (TSP), the company set goals to deliver high-quality software on time and within budget. In 2011, the company piloted AIM with positive results, and is now introducing it across the organization, with Kevin Davies, global director of technology, managing the implementation. “This initiative is not only improving how our IT organization functions, but will create greater transparency into IT for the whole company and provide a structured framework where all parties involved know what their responsibilities are and what they can expect,” said Davies.

Helping organizations implement AIM is one way the SEI promotes adoption of CMMI to achieve process performance results. AIM speeds CMMI adoption through a tailored version of TSP and Six Sigma measurement strategies. The AIM approach first focuses on appropriate training and gaining buy-in with senior management. It then works through the chain of command to middle- and first-line management, and finally to the developers who staff self-directed teams on initial AIM pilot projects.

When the AIM project pilots are complete, the focus moves to the organizational level through the use of TSP+ (a tailored form of TSP that incorporates elements from CMMI). TSP+ extends to the process group, which is responsible for CMMI implementation. AIM is then implemented project by project, instantiating the CMMI practices that apply to development projects.

Kathy Krauskopf, quality assurance manager for Urban Science, said, “Based on my experience in the past with CMMI (CMM at the time), I believed AIM would deliver process improvement benefits faster than the traditional IDEAL model. And this is what is happening.” Krauskopf noted that Urban Science has trained 30 developers in TSP fundamentals along with 24 leaders and team members, and has 3 pilots underway using TSP. With the help of an on-staff coach and a coach/TSP instructor, Urban Science now has three teams using TSP.

“Our experience with the SEI has been very positive,” said Krauskopf. “The SEI has done everything it can to make sure this is a success for us.”
“Urban Science is working to develop a whole new generation of web-based tools to support its analytics technology,” said Miluk. “This is a perfect example of a company searching for a better process technology and doing the necessary work to implement it.”

— GENE MILUK
The past year saw continued research by the SEI into addressing the challenges of monitoring large networks for malicious activity. The SEI’s approaches rely on techniques to summarize communications between hosts on the network. Even using summary techniques, monitoring large networks operated by the U.S. government and commercial enterprises generates huge volumes of data that security analysts cannot possibly analyze without assistance.

Network Situational Awareness (NetSA) team members in the SEI’s CERT® Program have developed approaches to automate that analysis. Both the U.S. Department of Homeland Security (DHS) and the Department of Defense (DoD) have applied these approaches to help security analysts monitor for unauthorized access of U.S. government networks and systems. In 2011, NetSA researchers developed new analytics, trained government personnel on their use, and delivered other resources to support Einstein, a capability used by the United States Computer Emergency Readiness Team (US-CERT), and Centaur, a capability used at the U.S. Cyber Command, the Defense Information Systems Agency (DISA), and the military services to defend DoD networks.

Aside from sheer volume, there are other challenges. For instance, organizations have traditionally monitored traffic at the perimeter of their networks. But well-defined, defensible network perimeters are being challenged by cloud computing, insider threats, and the prevalence of socially engineered application-level attacks over network-based attacks. Organizations are beginning to invest in and rely more on sensing outside of traditional network perimeters.
Members of the Secure Coding Initiative, part of the SEI’s CERT® Program, work with software developers and software development organizations to eliminate vulnerabilities resulting from coding errors before the software is deployed. In September 2011, Addison-Wesley Professional published *The CERT® Oracle® Secure Coding Standard for Java* by Fred Long, Dhruv Mohindra, and CERT researchers Robert C. Seacord, Dean F. Sutherland, and David Svoboda.

The standard developed out of a collaboration between the Secure Coding Team and Oracle’s Java platform developers. The Secure Coding Team also elicited feedback from the programming and software security community on proposed rules and recommended practices. The result is the first authoritative compilation of code-level requirements for secure Java systems.

“Conformance to these coding standards will allow developers to produce code that is free from those coding errors known to result in exploitable vulnerabilities,” said Seacord, the CERT team lead for secure coding. “We want to establish a set of rules that allow programmers to produce secure software and systems.” Seacord also noted that the secure coding standards establish a set of requirements for code security against which software can be evaluated.

*Secure Coding Standard for Java* joins the CERT Program’s coding standard for the C programming language as well as the C++ standard, which is in development.

Utility companies worldwide are using digital smart grid technology to modernize the aging analog power grid. Nearly 120 utilities have charted their smart grid strategies by using the Smart Grid Maturity Model (SGMM).

The SGMM is a management tool developed by utilities, stewarded by the SEI as part of its Smart Grid Initiative, and supported by the U.S. Department of Energy and many other stakeholders. Utilities use the SGMM suite of products to plan their smart grid implementation, prioritize their options, and measure their progress.

In September 2011, the SEI released Version 1.2 of the SGMM suite. Version 1.2 clarifies utility characteristics and explanations so that utility companies can more easily identify which areas of the model apply to them. The revised assessment survey allows participating utilities to better assess their smart grid progress against other utilities. Navigation workshops, in which SEI-Certified SGMM Navigators work directly with utilities, now provide improved guidance. Navigator training has also been made more efficient and effective, and licensing to deliver the Navigation Process has been opened to all qualified applicants.
More than 80 percent of the nation’s critical infrastructures are owned by private commercial organizations. The complexity and interconnectedness of networks and information technology that underpin these critical infrastructures make them hard to protect, and make it hard to measure their resilience. Cyber attacks on these networks and systems could adversely affect the national economy or government services, or could otherwise put the security of the United States at risk.
Partnership between the government and infrastructure owners and operators is an important factor in our national cyber security. Partnerships facilitate fast and effective communication about threats, vulnerabilities, and incidents. If needed, the government can assist in the response to cyber security incidents. This helps industry mitigate threats and protect its business. Partnerships also enable the government to understand changing information technology and industry’s security challenges.

The SEI participates in many initiatives that contribute to building public-private partnerships. For example, the Department of Defense (DoD) has an initiative to work more closely with the defense industrial base (DIB); that is, defense contractors, which often have sensitive but unclassified information on their enterprise networks. The goal of this initiative is to help them improve their ability to protect this information and respond to threats to its exposure. Information exchange enables both the DoD and its contractors to work more effectively and to act quickly if a security issue arises. The SEI is helping to establish a collaborative capability for government and industry partners to share information and for the industry partners to share information among themselves. The identity of industry partners is protected when they communicate with each other, promoting an anonymous, free flow of information even among competitors.

The SEI plays a similar role in a Department of Homeland Security (DHS) initiative to exchange information with critical infrastructure providers with the goal of enabling these providers to better secure the networks that the infrastructure relies on. Especially challenging is the need to determine how to help industry identify, respond to, and prevent attacks that commercial solutions do not yet detect and mitigate.

Another example of a public-private partnership is in the Cyber Resilience Review (CRR), which the DHS offers to critical infrastructure owners and operators. The approach was designed by the SEI, which helps with implementing the reviews. Based on the CERT Resilience Management Model, the CRR helps give a clear picture of an infrastructure’s security and resilience, along with improvement recommendations. More than a hundred CRRs have been conducted in sectors such as finance and energy. The ultimate goal of the public-private partnership is to help protect critical, privately owned national and economic assets.

Critical infrastructures are “those physical and cyber-based systems essential to the minimum operations of the economy and government. They include, but are not limited to, telecommunications, energy, banking and finance, transportation, water systems, and emergency services, both governmental and private.”

FROM PRESIDENTIAL DECISION DIRECTIVE 63
PUTTING THE CERT RESILIENCE MANAGEMENT MODEL INTO PRACTICE

CERT® Resilience Management Model (CERT-RMM) users have many resources for putting the model into practice: CERT-RMM Compass diagnostics, capability appraisals, users group workshops, and guidance on measuring progress. The CERT-RMM is the foundation for improving an organization’s ability to provide essential services in the presence of operational stress or disruption. In 2011, the CERT-RMM team built on its research to develop and launch the following products.

CERT-RMM Compass helps an organization quickly evaluate its resilience practices. This lightweight, questionnaire-based diagnostic is available for piloting and has been piloted in several organizations.

The CERT-RMM Capability Appraisal rigorously examines an organization’s implementation of resilience processes defined in the CERT-RMM. The SEI provides training, apprenticeships, and certification for lead appraisers. In 2011, 12 candidates started their apprenticeships, preparing to qualify as the first set of lead appraisers outside the SEI.

The CERT-RMM Users Group Workshop Series gives participants hands-on experience with applying the CERT-RMM. They prepare for each of four, two-day workshops with activities such as defining an improvement objective, using CERT-RMM Compass, preparing a presentation for management buy-in, and drafting an action plan. At each workshop, they report on their progress and get feedback from workshop leaders and other participants. Because the workshop enables participants to solve a problem in their own organization, the changes they implement become institutionalized—part of the way they do business. And the improvements in organizational practice resulting from the workshops pave the road for future improvements.

“CERT-RMM and the CERT-RMM Users Group guide me into assuring that my team is doing the right things in the right manner,” said Gregory Crabb, inspector in charge of Revenue, Product and Global Security, U.S. Postal Inspection Service. “Managing a security and resilience program can be challenging; participating in the Users Group gives me peace of mind that I am investing my limited resources in the most effective manner based on strong measurement and financial analysis.”

Echoing Crabb’s experience, Lockheed Martin’s Lynn Penn noted, “The CERT-RMM class provided Lockheed Martin participants with a solid framework for measuring organizational and operational resilience, but the RMM Users Group gave us a greater appreciation of the issues surrounding resilience.” Penn is director of strategic process engineering for Lockheed Martin. “The diversity of perspectives from industry, finance, government, and education helped to associate actual problems with model constructs,” she added. “Hearing about the real-world issues that other organizations had, and how they conquered or planned to conquer them, helped us to be better able to support our own operational teams and to establish a strategy for our organization.”

The CERT-RMM team also continued to pursue its research in the area of measurement, which is essential for all resilience-improvement efforts. Measures can indicate whether an organization is implementing the improved process and whether it makes a difference. To help CERT-RMM users select and apply resilience measures, the SEI is developing an initial set of resources, which currently include an approach, templates, and guidance that allows users to define measures tailored to their organizations’ needs.
“The CERT-RMM class provided Lockheed Martin participants with a solid framework for measuring organizational and operational resilience.”

—LYNN PENN, DIRECTOR OF STRATEGIC PROCESS ENGINEERING FOR LOCKHEED MARTIN

<table>
<thead>
<tr>
<th>MA</th>
<th>MON</th>
<th>OPD</th>
<th>OPI</th>
</tr>
</thead>
<tbody>
<tr>
<td>Measurement and Analysis</td>
<td>Monitoring</td>
<td>Organizational Process Definition</td>
<td>Significance Pre</td>
</tr>
<tr>
<td>PROCESS MANAGEMENT</td>
<td>DATA COLLECTION AND LOGGING</td>
<td>PROCESS MANAGEMENT</td>
<td>PROCESS MANAGEMENT</td>
</tr>
<tr>
<td>Develop and sustain a measurement capability that is used to support management information needs for managing the operational resilience management system</td>
<td>Collect, record, and distribute information about the operational resilience management system to the organization on a timely basis</td>
<td>Establish and maintain a set of organizational assets</td>
<td>Process Management</td>
</tr>
</tbody>
</table>
“Our protocol is the first one that allows multicore software to switch modes while meeting all timing requirements.”

— BJÖRN ANDERSSON
Advances in processor technology have shifted from faster processors to those that execute more instructions in parallel. These processors, called multicores, present challenges to software developers. Because multiple cores share memory, executing a function in one core can interfere with executing a function in another core. Stakeholders in the Department of Defense (DoD) and in industry fear multicore failure in systems such as aircraft and missiles, where lives are at stake.

Dionisio de Niz leads an SEI research effort to improve multicore processors. He explains that “for two cores performing two functions, execution times increase up to three times.” Arie Gurfinkel, a teammate of de Niz, adds that “the consequences of defects in mission-critical systems could be deadly, and the right answer delivered too late would become the wrong answer.” But the DoD will have to use multicores within 8 to 10 years, stressed team member Sagar Chaki, “because their ability to acquire single-core processors from chip manufacturers will run out.”

Multicore processors do provide benefits. For instance, with multicores, developers can make advantageous tradeoffs regarding size, weight, and power. “Unmanned aerial vehicles (UAVs) are getting smaller and more agile,” said de Niz, so they require more capabilities in fewer processors. Research, Technology, and System Solutions (RTSS) Program Director Linda Northrop noted that “multicore is the hardware of today, and it will be important for the DoD to exploit this technology.”

The team is investigating several challenges of multicore programming. It’s working on a technique using harmonic periods, which split task execution across two cores (migrating the task from one core to another) to prevent idle time in cores that cannot run a whole task. This maximizes the workload under strict deadlines and guarantees the same percentage of available processor capacity as in a single core.

SEI researcher Björn Andersson and collaborators from the Polytechnic Institute of Porto worked on software timing requirements. They developed a mode-change protocol for multicores with several operational modes, such as aircraft taxi, takeoff, flight, and landing modes. Andersson explained, “Our protocol is the first one that allows multicore software to switch modes while meeting all timing requirements. This lets software designers add or remove software functions while ensuring safety.”

The multicore team is also working on power optimization. “UAVs, robots, and smartphones run on batteries, and warfighters can perform longer missions if batteries last longer,” said team member Gabriel Moreno. Moreno and de Niz developed a new frequency-scaling algorithm that avoids processor partitions, so it can assign different speeds to individual cores. The method provides better power efficiency than was possible before.

Chaki and Gurfinkel worked on migrating real-time, embedded systems from single-core to multicore platforms. They want to apply regression verification to help enable this migration. Regression verification determines the behavioral equivalence of two related programs so that the computation effort of verification is proportional to the amount of difference between the programs rather than to their size.

Addressing the challenges of multicore programming is crucial to the DoD and industry, and the team’s work will help migration from single to multiple cores occur more safely and efficiently.
In March 2011, the National Science Foundation (NSF) selected 17 organizations, including Carnegie Mellon University (CMU), to partner on the Extreme Science and Engineering Discovery Environment (XSEDE) project. XSEDE is a five-year, $121-million effort aiming to create “the most advanced, powerful, and robust collection of integrated digital resources and services in the world.” XSEDE will build on the TeraGrid supercomputing network and provide researchers open access to state-of-the-art computational tools and digital resources. CMU’s team includes the Pittsburgh Supercomputing Center (PSC) and the SEI.

“On one level, we face a familiar challenge in introducing changes in engineering culture and practice: The computational science community supported by NSF and by XSEDE, has deep and varied technical expertise but lacks a sustainable sense of common engineering practice,” said Kurt Wallnau, senior member of the technical staff in the Research, Technology, and System Solutions (RTSS) Program at the SEI. “On another level, we face new challenges that stem from the need to think about computational science less as an amorphous community and more as a socio-technical ecosystem with institutional structures, niches, interests, and incentives. Thinking and working at ecosystem scale forces us to think about engineering in new and unfamiliar ways, but it also offers new opportunities to improve the scale, effectiveness, and adoption of software engineering practices.”

Wallnau noted that the SEI is playing a lead role in software development and integration on the project. It also holds leadership positions in the project’s systems engineering group, and it is contributing to the development of software architecture for XSEDE. “We’re working to fit all these things together,” said Wallnau.

The SEI XSEDE team also includes the following members of the technical staff: Felix Bachmann, Michael Gagliardi, Altaf Hossain, Scott Hissam, Mike Konrad, and Suzanne Miller. Joseph Batman and Paul Clements, both former members of the SEI staff, also contributed to this effort. The team sees great opportunity in this work. As Wallnau observed, “XSEDE gives us the opportunity to advance SEI research by understanding how these large, amorphous, distributed organizations work.”
SEI RESEARCH GROUP SEEKS MORE ACCURATE COST ESTIMATION

The difficulty of accurately estimating development costs for new Department of Defense (DoD) systems has been well documented, and cost overruns in new systems development are well known. This difficulty is compounded by the fact that estimates are now prepared much earlier in the acquisition lifecycle, well before there is concrete technical information available on the program to be developed. To address the challenge of accurate cost estimation, the Cost Estimation Research Group in the SEI’s Software Engineering Process Management Program developed a new approach, Quantifying Uncertainty in Early Lifecycle Cost Estimation (QUELCE).

QUELCE elicits information about program change-driver uncertainties common to program execution in a DoD major defense acquisition program lifecycle. It synthesizes analytical techniques such as scenario planning, Bayesian Belief Network (BBN) modeling, and Monte Carlo simulation into an estimation method that quantifies uncertainties, allows subjective inputs, visually depicts influential relationships among program change drivers and outputs, and assists with the explicit description and documentation underlying an estimate. “The innovation in this SEI solution rests with the desire to think out of the box from traditional parametric cost estimation,” said Robert Stoddard of the SEI’s Cost Estimation Research Group. “We’re tapping into other methods, such as scenario planning, to address the unique needs of early life-cycle cost estimation.”

The Cost Estimation Research Group detailed its work in the SEI technical report Quantifying Uncertainty in Early Lifecycle Cost Estimation (QUELCE). In addition to Stoddard, the group includes Robert Ferguson, Dennis Goldenson, James McCurley, and David Zubrow, all senior members of the SEI technical staff. The group looks forward to pilot applications of QUELCE by cost estimators in DoD environments.

40% RISE IN COST OVERRUNS ON DOD SYSTEMS PROJECTS, ACCORDING TO A RECENT GAO REPORT
“Our goal is to improve this process by introducing effective and automated scanning, and by preventing bad data from entering the system in the first place.”

— Mark Kasunic

$600 billion

According to a 2009 Gartner report, the annual cost of poor data to U.S. industry has been estimated at $600 billion.
Successful organizations understand the importance of measuring and analyzing data. They rely on data about their products, processes, and projects to make decisions and develop plans. But ensuring information quality is a big challenge for most organizations. In fact, they may not even be aware of just how good—or bad—their data are. And poor data quality leads to poor decisions.

Poor data quality is a pervasive problem in both industry and government. According to a 2009 Gartner report, the average organization loses $8.2 million annually because of poor data quality. The annual cost of poor data to U.S. industry has been estimated at $600 billion.

Government and industry both want to know: “How can we improve, evaluate, and standardize the quality of data we use?” To begin tackling this problem, SEI researchers collaborated with the Office of the Under Secretary of Defense (OSD) for Acquisition, Technology, and Logistics (AT&L), Acquisition Visibility (AV). The researchers, headed up by Mark Kasunic of the SEI’s Measurement and Analysis Team, set out to evaluate statistical methods for improving on existing, manual methods of anomaly detection. To do so, the team leveraged actual data in the Earned Value Management (EVM) Central Repository (CR). The EVM Central Repository supports the centralized reporting, collection, and distribution for key acquisition EVM data, such as Contract Performance Reports (CPRs), Contract Funds Status Report (CFSR), Integrated Master Schedule (IMS) for ACAT 1C & 1D (MDAP), and ACAT 1A (MAIS) programs.

The SEI team profiled and analyzed many months of EVM project data. It focused on identifying data anomalies involving cost estimates and performance values that seemed unusual when compared to the time-series values comprising the remainder of the data series. These unusual data values are considered outliers and tagged as anomalies. By creating graphic profiles of the data, the team uncovered anomalies that could be clearly observed as spikes or drops. The data-visualization methods appeared to be much more efficient and effective at identifying bad data than current methods.

“Once we discovered this, we consulted with our collaborator on our findings,” said Kasunic. “The findings were passed to a group of analysts to confirm whether the anomalies were of the type that the analysts would have flagged for further investigation.” Kasunic noted that the government does not have the staff to systematically evaluate large volumes of data; a systematic and automated way to screen data and discover data anomalies would lead to significant improvement, saving many analyst staff hours.

Checking the quality and accuracy of data is part of a process developed at the SEI called the Measurement and Analysis Infrastructure Diagnostic (MAID). MAID, which looks at the entire data life-cycle to ensure high quality, is a set of organized criteria that helps organizations discover the strengths and weaknesses of their information-measurement systems.

“Government analysts responsible for this do a tremendous job,” said Kasunic. “Our goal is to improve this process by introducing effective and automated scanning, and by preventing bad data from entering the system in the first place. The statistical methods we’ve applied have the potential to help them discover anomalies in the EVM system more quickly and with fewer resources. We hope this will ensure that information reported to Congress is highly accurate.”

Key Concepts of Earned Value Management
NORTHRUP NAMED SEI FELLOW

In 2011, Linda Northrop became an SEI fellow, a designation awarded to people who have made an outstanding commitment to the SEI and who continue to advise SEI leaders on key issues. Northrop, director of the Research, Technology, and System Solutions Program, is the fifth SEI fellow.

Northrop is the first woman to be named an SEI fellow and the first female program director at the SEI. “I have never been just the manager but have always been involved in research and technical work,” said Northrop. She originated the Framework for Software Product Line Practice, led a study of ultra-large-scale systems, and coauthored books on both topics.

Northrop’s leadership catalyzed widespread adoption of software product lines and software architecture. She believes that her work is “not so much about marketing products but about making a difference.” She founded the Software Product Lines Conference; forged the merger with its European counterpart, the Program Family Engineering Workshop; and initiated the SEI Architecture Technology User Network (SATURN) Conference.

Northrop has 35 years of experience in software engineering, more than 50 publications, and almost 300 presentations. Her honors include the New York State Chancellor’s Award for Excellence in Teaching, Carnegie Science Award of Excellence for Information Technology, and Association of Computing Machinery Distinguished Service Award. But for Northrop, the measure of her impact so far is leadership. “I loved being an educator,” she said, and she sees a similarity in her current role, in which, as program director, “I lead people to go further than I could go on my own.”

“I lead people to go further than I could go on my own.”

— LINDA NORTHRUP
In 2010, the SEI and Carnegie Mellon University (CMU) had the idea to create an innovation center, and in 2011, under sponsorship, developed a concept of operations (CONOPS) for a national innovation center. Today, SEI Innovation Center Director Matt Gaston says the center is tackling two challenges for the U.S. intelligence community and expects to expand.

WHAT IS THE VISION FOR THE SEI INNOVATION CENTER?

As part of a federally funded research and development center run by a university, we are working to become a mechanism that helps the government assess and leverage leading-edge technologies from the computing and information sciences for mission-critical cyber and intelligence needs. The world outside of government is innovating information technologies very rapidly. The government needs to keep pace. So, we are helping the government connect with innovative technologies and apply them to its work.

The Center can do this in two key ways: by providing a view into research to identify solutions and make them relevant and, on the mission side, by working with customers on their greatest mission challenges. To borrow a phrase from Randy Bryant (dean of Carnegie Mellon’s School of Computer Science): Our technical focus area is data-intensive scalable computing. We work on the question “How do we bring innovation to bear on real government challenges?”

WHAT HAS HAPPENED SINCE YOU FINALIZED THE CONOPS FOR THE SEI INNOVATION CENTER?

In our inaugural year, we’ve secured two major sponsors and two major projects. In the first project, we are supporting the efforts of our sponsor to move to the cloud. In particular, we’re helping with various aspects of heterogeneous high-performance computing (HPC) utility clouds. That sponsor has given us funding to purchase an instance of their infrastructure, which we will stand up at the SEI for research and development use. Our research will focus on using HPC utility clouds to dynamically provision mission applications that require a great deal of computing power and resources onto a common infrastructure.

Our second sponsor funded an unclassified cyber-intelligence pilot aimed at increasing awareness of network activity, and cyber threat activity, in the private sector. We are taking information from commercial and open-source providers and fusing it into a more complete picture of current activity. We’re then providing a reporting stream back to the private sector. This establishes an intelligence testbed for technologies and techniques used for processing, analyzing, and reporting on a lot of information.

One of the assumptions going into all of our work was that the SEI Innovation Center would focus on building prototype technology capability; in other words, on building software, not thinking about software or processes or engineering, but actually doing software.

DO YOU CONNECT WITH OTHER PARTS OF THE SEI AND CAMPUS?

Collaboration is very much a part of the SEI Innovation Center’s approach. Though we are in the formative stages, we are managing our growth and establishing collaborative ties with all the SEI technical programs, and we are actively looking for projects on which we can work together. We are also looking at appropriate mechanisms to collaborate closely with the CMU campus. While we refine these mechanisms, we’re building relationships with the School of Computer Science and the Carnegie Institute of Technology.
“We’ve gotten feedback from people saying that this kind of hands-on, experiential learning ‘will be incredibly helpful to DoD program offices.’”

— BILL NOVAK

90% THE “90 PERCENT SYNDROME” OFTEN EMERGES IN THE LATE STAGES OF DEVELOPMENT WHEN PROGRESS ON THE EFFORT SEEMS TO STALL AT APPROXIMATELY 90% DONE, AND THEN INCHES SLOWLY FORWARD TO EVENTUAL COMPLETION.
ACQUISITION MODEL TO HELP PROGRAM OFFICES AVOID COMMON PITFALLS

An acquisition project starts with the best intentions: to field a high-quality system that provides new or improved capabilities to the warfighter. Unfortunately, somewhere between the prototype and deployment of the finished system, the effort goes awry, and the system, as initially envisioned, takes much longer than expected, or may never come to fruition.

The problem is common enough that SEI researchers aggregated work on five independent technology assessments (ITAs) from 2006-2009 to develop a model of this acquisition scenario, which they titled “The Evolution of a Science Project.” The scenario goes like this: A project begins with an informal team of operational people building a small, throwaway, proof-of-concept prototype to solicit funding. A successful initial deployment of the prototype builds demand for more capabilities and broader deployment. The project builds on top of the initial prototype to save time, but then starts to find increasing architectural, robustness, performance, usability, and documentation issues. As developers spend more time supporting field users, development progress slows. A lack of either project management experience or a formal organization also creates problems as developers try to scale the effort up into a formal program, resulting in a difficult transition as warfighters wait years for a production-quality system.

Bill Novak, senior member of the SEI technical staff with the Acquisition Support Program, noted that there are at least two dynamics at work behind the scenes in this scenario. “First, the project is often initiated by operational users who may lack software acquisition expertise,” Novak said. “They focus primarily on quick deployment and operational support, which can result in informal requirements, poor design and code quality, and inadequate documentation.”

The second dynamic is called “firefighting.” “People who are slated to do new development of the next release must be diverted to fix problems in previously fielded releases,” said Novak. “This not only slows new development, but the lack of developers can inject additional problems in the next release that will require even more people to fix.”

Andy Moore, from the Enterprise Threat and Vulnerability Management team in the CERT Program, described a couple of preliminary findings from the modeling effort. “The accumulation of undiscovered rework from development of the science project prototype moves the development efforts past a tipping point of escalating repair work during the follow-on development.” The tipping point was found to contribute to the “90 Percent Syndrome” experienced in many software development efforts, causing the program to shift from completing normally, to having defects accumulate as rapidly as they can be corrected. Moore commented that “this syndrome occurs during the later stages of development when progress drastically slows down as a much bigger percentage of the effort is devoted to repair work rather than development.”

Some of the key factors behind reaching the tipping point include

- excessive pressure being applied to the developers
- an emphasis on meeting schedule, rather than on quality
- the timing of the transition from prototype to production development (an earlier transition has fewer undiscovered defects in it)

“These are preliminary findings, as we will be performing additional model validation in the coming year,” Novak pointed out, while observing that, “the model’s qualitative behavior is similar to what we observe in actual programs.”

The SEI’s work to date on the project will be captured in an upcoming technical report: The Evolution of a Science Project: System Dynamics Modeling of a Recurring Software-Reliant Acquisition Behavior. The team also plans to create an interactive classroom game based on the model to teach better decision making for the defense acquisition workforce that can help lead to better program outcomes. “We’ve gotten feedback from people saying that this kind of hands-on, experiential learning will be incredibly helpful to DoD program offices,” said Novak.
CERT EXERCISE NETWORK (XNET) INSTRUMENTAL IN SUCCESSFUL TEST OF CYBER ATTACK READINESS

In May 2010, leaders of the U.S. Cyber Command had a problem: Where could they find a range to run cyber defense exercises involving a complex scenario, dozens of simulated but realistic networks, and participants scattered across the Department of Defense (DoD)? And could that range be ready in record time? They found their solution at the SEI, which developed the CERT Exercise Network (XNET)—a next-generation cybersecurity training and simulation platform for realistic, scalable, scenario-driven cybersecurity exercises.

XNET provided the range, the instrumentation, and the thousands of virtual computers needed for Cyber Command’s week-long exercise called Cyber Flag 12-1. The exercise involved more than 300 participants from across the DoD who worked together to detect and respond to real-world cyber threats on a virtualized network topology like their own.

Jeff Mattson, who managed the SEI’s XNET development team, described the challenge of running useful exercises: “You want to be able to train as you fight. You can’t play war games on your production network without risking potential damage. XNET provided a large, complex, highly instrumented network that allowed Cyber Command to run realistic cyber threat, defense, and response operations.”

In addition to high fidelity, XNET offers a highly extensible and dynamic environment that allows organizations to start, stop, and reset the network resources on the fly. “You can easily manipulate the XNET environment,” said Chris May, technical manager for the CERT Program’s Cyber Workforce Development Team. “Unlike more monolithic ranges, we could dynamically change the environment based on the conditions in the scenario.”

The Cyber Flag exercise used a variety of scenarios based on likely adversary actions in real-world events. Participants were split into two teams to practice offensive and defensive tactics. Opposing forces tried to infiltrate Cyber Command’s virtual network using malware and other forms of network intrusion.

Air Force Lt. Col. William Hutchison, who led the Cyber Flag exercise, saw value in the results: “Exercises like Cyber Flag are important because they provide an assessment and a validation of how well U.S. Cyber Command can perform its real-world mission to operate and defend the DoD networks across the full range of cyber operations.”

Mattson’s team worked in record time. It had the Cyber Flag range environment up and running in only 6 months—much faster than the 18 months typically required for planning and development. Hutchison described the team’s work this way: “Only a select few in the community believed the XNET team could accomplish what they did in the needed, high-risk timeframe. We put our faith in May, his team, and the XNET product, and they exceeded our expectations.”

Because the Cyber Flag exercise was such a success, U.S. Cyber Command plans to run one every year, and May has a new goal for XNET. “Next year, we want to raise the level of fidelity even further—enabling commanders to validate the mission-readiness of units or teams that have to support real-world operations. They want to use XNET to train and verify that they can accomplish the DoD’s cyber mission under any conditions. XNET can help them do just that.”
Exercises like Cyber Flag are important because they provide an assessment and a validation of how well U.S. Cyber Command can perform its real-world mission to operate and defend the DoD networks across the full range of cyber operations."

—AIR FORCE LT. COL. WILLIAM HUTCHISON
SEI PROFESSIONAL DEVELOPMENT CENTER

The SEI Professional Development Center incorporates education, training, and credentials, all of which enable individuals to benefit from SEI research in multiple disciplines.

The center provides continuing education for engineering and software professionals in government, industry, and academia.

THE SEI ADDRESSES PROFESSIONAL DEVELOPMENT NEEDS BY

• designing and developing training that is accessible and effective with classroom, blended, and distance learning
• encouraging and recognizing individual accomplishments in various disciplines through certificate programs
• enhancing individual career opportunities through SEI Certification

FOR MORE INFORMATION ABOUT SEI TRAINING, VISIT www.sei.cmu.edu/training

FOR MORE INFORMATION ABOUT SEI CERTIFICATION, VISIT www.sei.cmu.edu/certification

SEI CONFERENCES & EVENTS

As part of its strategy to apply the latest research, the SEI offers conferences, workshops, and user-group meetings. These events represent technical work and research performed by the SEI and its collaborators in the areas of process improvement, software architecture and product lines, security, acquisition, and interoperability. Individuals from around the world attend SEI conferences and events to

• connect with industry leaders
• share best practices
• network with peers
• find potential solutions
• gather the latest research and trends in software and systems engineering

SOME OF THE EVENTS THAT THE SEI SPONSORED AND CO-SPONSORED IN 2011 ARE

• CMMI Workshop 2011
• FloCon 2011
• SATURN 2011
• SEPG North America 2011

FOR MORE INFORMATION ABOUT SEI CONFERENCES AND EVENTS, VISIT www.sei.cmu.edu/events

SEI PARTNER NETWORK

The SEI Partner Network is an elite group of SEI-trained organizations on the leading edge of software engineering processes and technologies. SEI Partners are licensed to deliver SEI services in the following areas:

• Architecture Tradeoff Analysis Method
• CERT Information Security
• CMMI and SCAMPI Appraisals
• People Capability Maturity Model
• Service-Oriented Architecture
• Smart Grid
• Software Architecture
• Software Engineering Measurement and Analysis
• Team Software Process

By delivering services worldwide, SEI Partners provide a critical distribution channel for accomplishing the SEI mission.

In fiscal year 2011, the SEI Partner Network consisted of 448 Partner organizations.

FOR MORE INFORMATION ABOUT THE SEI PARTNER NETWORK, VISIT www.sei.cmu.edu/partners

SEI AFFILIATE PROGRAM

Through the SEI Affiliate Program, sponsoring organizations contribute technical staff members to the SEI’s ongoing effort to define superior software and systems engineering best practices. Affiliates lend their technical knowledge and experience to SEI teams investigating specific technology domains.

Affiliates are immersed in the inquiry and exploration of new tools and methods that promise to increase productivity, make schedules predictable, reduce defects, and decrease costs.

FOR MORE INFORMATION ABOUT THE SEI AFFILIATE PROGRAM, VISIT www.sei.cmu.edu/careers/affiliates
# LEADERSHIP, MANAGEMENT, & STAFF

## SEI 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.

<table>
<thead>
<tr>
<th>Name</th>
<th>Title</th>
<th>Experience</th>
</tr>
</thead>
<tbody>
<tr>
<td>ALAN J. MCLAUGHLIN</td>
<td>Chair, Board of Visitors Consultant; Former Assistant Director</td>
<td>MIT Lincoln Laboratory</td>
</tr>
<tr>
<td>BARRY W. BOEHM</td>
<td>TRW Professor of Software Engineering University of Southern California; Director University of Southern California Center for Software Engineering</td>
<td></td>
</tr>
<tr>
<td>CLAUDE M. BOLTON</td>
<td>Executive-In-Residence, Defense Acquisition University of the Army for Acquisition, Logistics, and Technology</td>
<td></td>
</tr>
<tr>
<td>WILLIAM BOWES</td>
<td>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</td>
<td></td>
</tr>
<tr>
<td>CHRISTINE DAVIS</td>
<td>Consultant; Former Executive Vice President, Raytheon Systems Company</td>
<td></td>
</tr>
<tr>
<td>GILBERT F. DECKER</td>
<td>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</td>
<td></td>
</tr>
<tr>
<td>PHILIP DOWD</td>
<td>Private Investor; Former Senior Vice President, SunGard Data Systems; Trustee, Carnegie Mellon University</td>
<td></td>
</tr>
<tr>
<td>TOM LOVE</td>
<td>Chief Executive Officer, ShouldersCorp; Founder of Object Technology Group within IBM Consulting</td>
<td></td>
</tr>
<tr>
<td>DONALD STITZENBERG</td>
<td>President, CBA Associates; Trustee, Carnegie Mellon University; Former Executive Director of Clinical Biostatistics at Merck; Member, New Jersey Bar Association</td>
<td></td>
</tr>
<tr>
<td>JOHN M. GILLIGAN</td>
<td>President, Gilligan Group; Former Senior Vice President and Director, Defense Sector of SRA International; Former CIO for the Department of Energy</td>
<td></td>
</tr>
</tbody>
</table>
The SEI Director’s Office leads the Institute’s research program and ensures the smooth, efficient operation of the SEI. Director and Chief Executive Officer Paul Nielsen builds strong, collaborative relationships with leaders in government, industry, and academia, communicating the SEI’s vision for software engineering.

PAUL D. NIELSEN
Director & Chief Executive Officer

PETER MENNITI
Acting Chief Operating Officer
Director, Financial and Business Services
SEI MANAGEMENT

The SEI Management Team comprises the directors of the research programs, technology transition, and business and technology functions of the SEI.

JOHN BRAMER  
Director, Program Development and Transition

ANITA CARLETON  
Director, Software Engineering Process Management

LINDA NORTHROP  
Director, Research, Technology, and System Solutions

RICHARD PETHIA  
Director, Networked Systems Survivability

TERRY ROBERTS  
Executive Director, Acquisition Support Program/Interagency and Cyber

DAVID THOMPSON  
Director, Information Technology and Security
KEY PUBLICATIONS

ARTICLES


Moore, Andrew P.; Cappelli, Dawn M.; Caron, Thomas C.; Shaw, Eric; Spooner, Derrick & Trzeciak, Randall F. “A Preliminary Model of Insider Theft of Intellectual Property.” Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA) and SEI 2, 1 (March 2011): 28-49.


BOOKS & BOOK CHAPTERS


KEYNOTES


Nielsen, Paul D. Lean Software & Systems Conference (May 2011)

Over, James. “Failure Is Not an Option,” TSP Symposium (September 2011) and SEPG Europe 2011 (June 2011)

Place, Pat. “SOA and the Cloud: SEI Perspective,” SOA, Cloud Computing, and Virtualization (May 2011)


PODCASTS & WEBINARS


WORKSHOPS & TUTORIALS


**KEY PUBLICATIONS**


Mondragon, Oscar & Willett, Alan. “Applying TSP for Services: Seven Key Lessons Learned.” TSP Symposium 2011, Atlanta, GA (September 2011).


Young, Rawdon; Penn, Mary Lynn & Hayes, Will. “CMMI Version 1.3 High Maturity—We Thought but Now We Know.” SEPG North America 2011, Portland, OR (March 2011).


SEI REPORTS (UNLIMITED DISTRIBUTION) PUBLISHED 01 OCT 2010 - 30 SEP 2011


Anderson, William; Andrews, Archie D.; Brown, Nanette; Cohen, Cory; Craig, Christopher; Daly, Tim; de Niz, Dionisio; Diaz-Pace, Andres; Feiler, Peter H.; Fisher, David; Gluch, David P.; Hansen, Jeffrey; Hanson, Jörgen; Hudak, John J.; Lakshmanan, Karthik; Linger, Richard C.; Lipson, Howard F.; Moreno, Gabriel; Morris, Edwin J.; Mutlu, Onur; Nord, Robert; Ozkaya, İpek; Plakosh, Daniel; Pleszkoch, Mark; Rajkumar, Ragunathan; Seibel, Joe; Simanta, Soumya; Weinstock, Charles B. & Wragé, Lutz. Results of SEI Independent Research and Development Projects. www.sei.cmu.edu/library/abstracts/reports/11tr002.cfm


Chaki, Sagar; Creel, Rita C.; Davenport, Jeff; Kinney, Mike; McCormick, Benjamin & Popeck, Mary. Standards-Based Automated Remediation: A Remediation Manager Reference Implementation. www.sei.cmu.edu/library/abstracts/reports/11sr007.cfm

CMII Product Team. CMMI for Acquisition, Version 1.3. www.sei.cmu.edu/library/abstracts/reports/10tr032.cfm

CMII Product Team. CMMI for Services, Version 1.3. www.sei.cmu.edu/library/abstracts/reports/10tr034.cfm

CMII Product Team. CMMI® for Development, Version 1.3. CMMI-DEV/V1.3. www.sei.cmu.edu/library/abstracts/reports/10tr033.cfm
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 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 that want to develop a strategic advantage by rapidly applying improved software engineering technology.

The SEI works with organizations that want to combine their expertise with the SEI’s expertise to mature new technology for the benefit of the entire software industry. The SEI also supports a select group called SEI Partners, which are organizations and individuals trained and licensed by the SEI to deliver SEI products and services.

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 staff divisions. Contact the SEI Human Resources department to learn about the benefits of working at the SEI: www.sei.cmu.edu/careers