20
06 Annual Report

Intellectual Capital
Shaping the Future of Software Engineering

Software Engineering Institute | Carnegie Mellon

Software Engineering Institute | **Carnegie Mellon**

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 advances software engineering and related disciplines to ensure the development and operation of systems with predictable and improved cost, schedule, and quality.

As the only FFRDC focusing on software engineering, the SEI must have a staff that is technically excellent. The stories that begin on page 7 exemplify how the people of the SEI advanced the field of software and systems engineering during the fiscal year that ended September 30, 2006.

Message from the Director

At the Software Engineering Institute, our most important assets are our people.
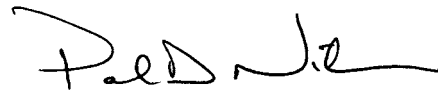
Some organizations say this, but don't mean it. Other organizations mean it, but don't act like it. To be a great science and technology organization, you have to mean it—and act like it.

The SEI's product is the knowledge we create and capture, apply to real-world problems, and distribute to the global software and systems engineering community. This product comes from only one source—our people. We depend on our men and women to innovate, to collaborate with researchers throughout the world, to synthesize ideas from many fields, to refine new methods and techniques for producing world-class software and systems and, ultimately, to transfer these methods and techniques to the broad software community.

In this year's annual report, we profile people at the SEI whose contributions are shaping the future of software and systems engineering. They take different approaches to this challenge. Sagar Chaki and his colleagues examine formal methods that enable engineers to assemble large software systems from trusted, certifiable components. Tom Longstaff surveys the digital universe to understand the myriad ways that people create value online, with the goal of keeping one step ahead of those who would steal or destroy that value.

Although they may work at diverse points along the full spectrum of software engineering, our people share a common vision: that software has the potential to enrich society. In short, our people want to make the world better.

While they share a vision, they are also an extraordinarily diverse group: a former agent with the Drug Enforcement Agency, an engineer with a degree in diplomacy, a sociologist, a foreign correspondent. Their backgrounds and personal stories paint an image of the vibrant, exciting, and stimulating world of the SEI. We invite you to learn more about the SEI and the people who, every day, help lead us to a software-enriched future.

Strategy

SEI staff members achieve the goals of the institute through technology innovation and transition. They create usable technologies, apply them to real problems, and amplify their impact by accelerating broad adoption.

Create

The SEI addresses significant and pervasive problems in software engineering and related disciplines by
- motivating research
- developing innovative new technologies
- identifying and fostering the development and improvement of emerging or underused technologies
- improving and adapting existing solutions

SEI technologies and solutions are suitable for all organizations that commission, build, or use systems that depend on software.

The SEI collaborates with innovators and researchers to implement these activities.

Apply

Because application and validation are required to prove effectiveness, applicability, and transition potential, the SEI applies, validates, refines, and extends new and improved technologies and solutions in real-world government and commercial contexts. Refining and extending technologies and solutions is an intrinsic part of application.

Government and commercial organizations directly benefit from these engagements. In addition, the experience that SEI staff members gain through these engagements helps to identify
- real-world problems that warrant further investigation in the Create phase
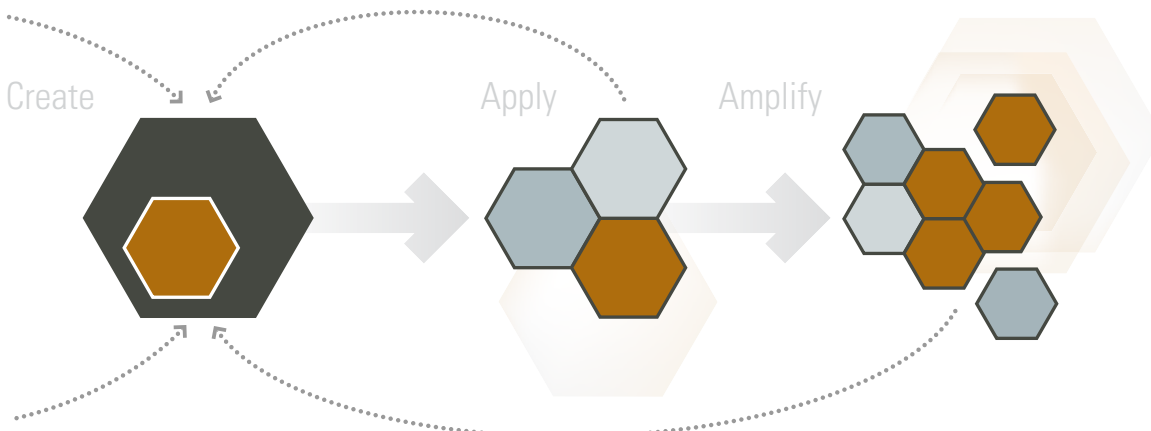- needed transition artifacts and strategies for encouraging and supporting adoption in the Amplify phase

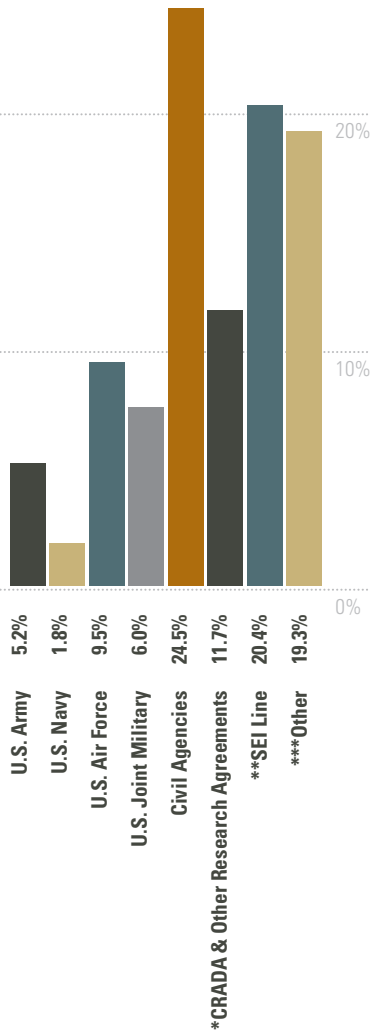The SEI works with early adopters to implement these activities.

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
- courses
- licenses for use and delivery
- authorizations and certifications
- workshops and conferences
- leadership in professional organizations
- Web-based communication
- books and publications
- advocacy

Professionals throughout the world accelerate the adoption and impact of software engineering improvements through direct interaction with the SEI and with SEI Partners—organizations and individuals licensed by the SEI to deliver SEI services.

Create   Apply   Amplify

Areas of Work

The SEI technical program—created and carried out by world-recognized leaders in software engineering, security, and process improvement—consists of five technical focus areas. The SEI also conducts new research into emerging topics in software and systems engineering.

For 22 years, the Carnegie Mellon® Software Engineering Institute has served the nation as a federally funded research and development center. The SEI staff has advanced software engineering principles and practices and has served as a national and international resource in software engineering, computer security, and process improvement. As part of the world-renowned Carnegie Mellon University—a global research university of more than 10,000 students and more than 4,000 faculty and staff—the SEI and its staff operate at the leading edge of technical innovation.

The SEI's technical focus areas together with its outreach activities are aimed at meeting the defined software engineering needs of the U.S. Department of Defense. Within these areas of work, the SEI collaborates with defense, government, industry, and academic institutions to continuously improve software-intensive systems.

20%

10%

0%

U.S. Army	5.2%
U.S. Navy	1.8%
U.S. Air Force	9.5%
U.S. Joint Military	6.0%
Civil Agencies	24.5%
*CRADA & Other Research Agreements	11.7%
**SEI Line	20.4%
***Other	19.3%

SEI Funding by Organization

In FY 2006, the SEI received $100.3 million in funding from a variety of sources.

* cooperative research and development agreement—an agreement with an industry or an academic collaborator

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

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

Acquisition

Support for the DoD, federal agencies, and others in institutionalizing and continuously improving their ability to acquire, deploy, and sustain systems that meet cost, schedule, and technical objectives.

Architecture, Product Lines, & Predictable Assembly

Practices and techniques for predictably and efficiently designing, constructing, and guiding the evolution of software-intensive systems with the qualities needed to meet business and mission goals.

Process Improvement & Performance Measurement

Process-management practices and performance-improvement and measurement techniques for software and related disciplines in support of the management, development, and acquisition of software and systems.

Security

Technologies, system-development practices, and system-management practices that can significantly improve networked systems security and survivability. Includes CERT, a center of Internet security expertise.

System Interoperability, Performance, & Dependability

Technology and practices to achieve system-of-systems interoperability and to predict and improve the performance and dependability characteristics of embedded and large systems.

> "The SEI's product is the knowledge we create and capture, apply to real-world problems, and distribute to the global software and systems engineering community.
>
> This product comes from only one source—our people."
>
> —Paul Nielsen

Intellectual capital

Sixteen stories about our people

16

Planning for Ultra-Large-Scale Systems: The Software Challenge of the Future

"The difference in scale between today's largest systems and the systems that we will build in the future is like the difference between constructing buildings and guiding the growth and evolution of cities," says Linda M. Northrop, director of the SEI Product Line Systems Program.

Northrop's analogy to a city can be extended to her own leadership of the ultra-large-scale (ULS) systems study. Under Northrop's leadership, the SEI in FY 2006 assembled experts from within and outside the field of software engineering to study ULS systems—systems whose large size along multiple dimensions makes constructing them problematic. Northrop's role in coordinating the efforts of this diverse group was more like that of the mayor of a large city than of a building architect. With a combination of vision, diplomacy, accommodation, consensus-building, persuasion, and political savvy, Northrop led the team to produce *Ultra-Large-Scale Systems: The Software Challenge of the Future*, which describes a multidisciplinary, forward-looking research agenda to deal with the ULS systems in our future.

For Northrop, leading the ULS systems study represents the latest achievement in a distinguished career that began in software development and education. As a software engineer at IBM and Eastman Kodak and as a private consultant, she acquired experience in designing and building software systems. As a tenured computer science professor at the State University of New York College at Brockport, she developed an early research interest in object technology and explored educational models for designing and teaching courses in software engineering.

After two years as a distinguished visiting professor at the U.S. Air Force Academy, Northrop came to the SEI to help develop software engineering curricula for undergraduates, graduates, and professionals. Taking advantage of her expertise in object technology, the SEI also enlisted Northrop as a member of SEI teams conducting independent technical assessments of government programs. In 1995, she was named director of the SEI Product Line Systems Program.

When Claude M. Bolton, Jr., asssistant secretary of the U.S. Army (Acquisition, Logistics, & Technology), posed a challenge to the SEI—"Given the issues with today's software engineering, how can we build the systems of the future that are likely to have billions of lines of code?"—SEI management turned to Northrop.

"As framed by Mr. Bolton, the ULS problem called for innovative thinking from a broad range of disciplines," she says. "During my years at the SEI, I have stayed connected to the object community, and I have also maintained relationships with key academic researchers. These extracurricular activities gave me access to a wide array of influential thinkers."

Northrop brought together experts in the social sciences, economics, human interfaces, security, reliability, real-time performance, and programming languages. The team's report has received widespread attention and praise since its publication in July 2006. "Linda's competence and leadership were critical to accomplishing the mission," says Assistant Secretary Bolton. "She provided the vision and enthusiasm deserving of the ULS challenge."

> " The difference in scale between today's largest systems and the systems that we will build in the future is like the difference between constructing buildings and guiding the growth and evolution of cities. "

LINDA NORTHROP

The principal team of authors who wrote the *Ultra-Large-Scale Systems* report consisted of Peter Feiler, John Goodenough, Rick Linger, Tom Longstaff, Rick Kazman, Mark Klein, Linda Northrop, and Kurt Wallnau from the SEI, along with Richard P. Gabriel, Sun Microsystems, Inc.; Douglas Schmidt, Vanderbilt University; and Kevin Sullivan, University of Virginia. Bill Pollak was the principal editor, and Daniel Pipitone was the lead graphics and layout designer.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16

www.sei.cmu.edu/uls

1

3

SAGAR CHAKI

4

5

6

7

8

9

10

11

12

How can you trust that a software system, assembled from various third-party components, will do what you expect it to do, and that nothing bad will ever happen?

13

14

15

16

Research on Binaries Points Way to Building Trustworthy Software from the Ground Up

How can you trust that a software system, assembled from various third-party components, will do what you expect it to do, and that nothing bad will ever happen? One way, says Sagar Chaki, is to establish proof of correctness at the most fundamental level of software, the binary, and build up from there.

Chaki and his fellow researchers at the SEI and Carnegie Mellon University have employed the concept of proof-carrying code on two consecutive research projects. The essential idea of proof-carrying code is to construct a proof of the claim that a piece of machine code respects a desired policy—that "something bad never happens," for example, or that "something good will eventually happen." The proof is shipped along with the code in the form of a compact certificate so that it can be independently verified before the code is deployed.

"As software becomes more pervasive and more complex, we need a mechanism to ensure correctness," Chaki says. "With proof certificates, we can show not just why a program is buggy, but why a program is correct."

In the first project, in 2005, the team members developed an infrastructure to generate compact certificates for programs written in C. In 2006, they extended that framework to certify binaries generated from component specifications. This project completed the framework for proof-carrying code. The next step is to find a suitable partner to pilot the approach.

Chaki and his colleagues are working at the forefront of predictable assembly, and Chaki is comfortable at the head of the class. His meteoric academic career began in the Calcutta suburb of Barasat, where Chaki, the son of an engineer, happily found that he shared his father's knack for math and science.

"In India, there is a hierarchy of fields. Most people I grew up with aspired to become either a doctor or an engineer," he says.

He chose engineering, and scoring in the top 2 percent of students on the university entrance exams gained him admission to the Indian Institute of Technology in Kharagpur in 1995. From there, he branched into the emerging field of computer science. After graduating at the top of his class and winning the prestigious President of India Gold Medal, he left India to earn his PhD at Carnegie Mellon. His PhD thesis in formal software verification meshed with related work at the SEI, and Chaki collaborated on SEI projects as a student before joining the institute upon receiving his PhD in January 2005.

With the early phases of research complete on certification and verification, Chaki looks forward to a day when the approach achieves mainstream use. He compares today's software climate to the mid-1990s, when the hardware industry embraced model checking as a way to find flaws in microprocessors. "There are a lot of small but critical software components that we use out of habit and just trust," Chaki says. "But widely publicized software glitches continue to occur, and commercial formal software-verification tools are already available. I believe this trend is going to gain momentum, and formal software certification will become an important part of the picture."

Team Studies Risk Indicators in Joint Capabilities

David Zubrow gave the U.S. Department of Defense (DoD) some troubling news in 2006 about joint capabilities. The DoD wants to estimate costs for joint capabilities as accurately as it does those for individual weapons systems. A joint capability enables service operations to meet nontraditional threats and requires individual systems to work together.

Zubrow's SEI team found that the DoD needs, but does not receive, assessments with adequate leading indicators of cost and schedule breaches for joint capabilities, particularly those related to technology development. This important finding leads toward understanding more about how programs relate to one another. "We were able to say, 'Here's what's going on from a joint capabilities view,'" Zubrow says.

Zubrow's work is being sponsored by the Office of the Secretary of Defense Program Analysis and Evaluation (OSD/PA&E) and the Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics (OUSD/AT&L).

"We're another instrument in a larger effort to get a handle on something that is unprecedented from a DoD acquisition perspective," Zubrow says of his team. In all, Zubrow's team developed a risk taxonomy, a set of diagnostic risk indicators, and a case study in 2006. The case study used data from the Multifunctional Information Distribution System–Low Volume Terminal (MIDS-LVT) program. Service branches and allied forces will depend on MIDS-LVT for surveillance, identification, air control, weapons engagement coordination, and direction.

An expert in management, quality, and analysis, Zubrow approached the research challenge deftly. Zubrow says that he matched his team to the "parts of the challenge—cost measurement and interoperability." He recruited a multidisciplinary team including SEI staff members James McCurley, an expert in measurement and analysis, and William Anderson, an expert in interoperability. He and the sponsor also engaged Mary Maureen Brown from the University of North Carolina and researchers from Technomics, Inc., an organization experienced in cost estimation.

Anderson worked with the research sponsor to collect data and formed the taxonomy of risk indicators, leveraging Brown's work and SEI software development and acquisition risk taxonomies. McCurley painstakingly mined the MIDS-LVT data, burrowing through it for clues that might predict cost and schedule breaches. In the past, McCurley has analyzed multifaceted problems in such diverse areas as energy production, water quality, pollution control, and cyber security. "I like to work on complex problems," McCurley explains. "The challenge is what drives me."

To sum up his approach to managing the team, Zubrow echoes leadership expert W. Edwards Deming: "Create constancy of purpose toward improvement." Zubrow's SEI career is punctuated with other examples of his own constancy of purpose toward improvement. He was instrumental in creating a system to make process maturity profiles widely available, for instance. Also, he established a training curriculum that addresses the needs of a broad spectrum of measurement and process improvement audiences.

Zubrow's team will continue to work with the PA&E and AT&L sponsors. "We are unavoidably moving toward systems of systems," Anderson says. "We have to get a better handle on what it takes to get them to interoperate. When our systems fail to interoperate, we're at risk, and our costs are higher."

> " We are unavoidably moving toward systems of systems. We have to get a better handle on what it takes to get them to interoperate. When our systems fail to interoperate, we're at risk, and our costs are higher "
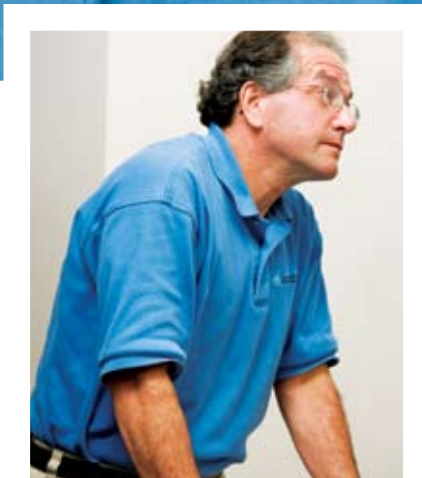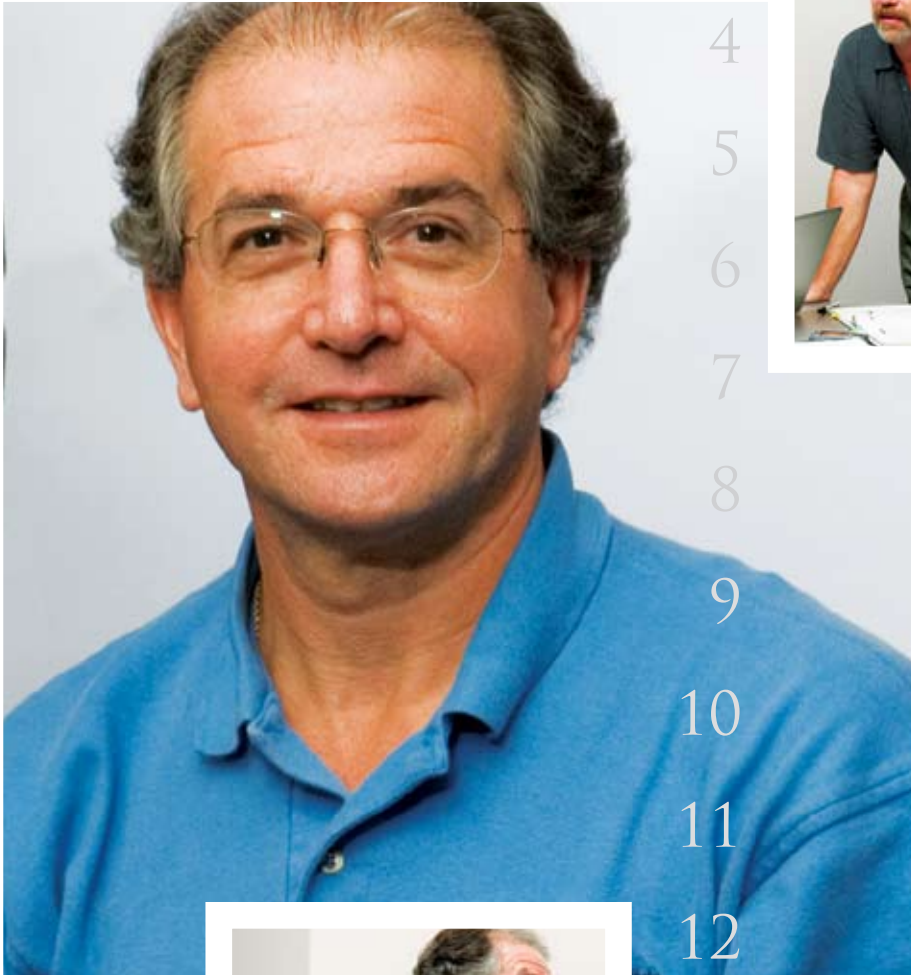
James McCurley and William Anderson

DAVID ZUBROW

Lutz Wrage

Soumya Simanta

Lewis's teammates Lutz Wrage and Soumya Simanta gravitated toward the TechCheck work because of their experience in software development and technology evaluation. Wrage revels in examining real-world technology issues. From his days up-grading an enterprise resource-planning system and assessing software as a consultant and entrepreneur to the TechCheck work, Wrage has seen that a deep-level evaluation of new technologies is vital. "You cannot find out enough about a technology just by reading about it," Wrage says.

Simanta joined the TechCheck effort after several years of developing distributed systems for commercial organizations. He also obtained a master's degree from Carnegie Mellon University, where his mentor was Lewis. The TechCheck ap-proach, Simanta points out, "makes the best use of limited evaluation resources" to help an organization "identify risks and find solutions for problems before they become too difficult to handle effectively."

1
2
3

GRACE LEWIS

4
5
6
7
8
9
10
11
12

13 "Before commenting on technologies that promote interoperability, we have to
14 know what they can do and what they cannot do."

15

16

New Approach Reveals Gaps in Interoperability Tools

"Before commenting on technologies that promote interoperability, we have to know what they can do and what they cannot do," Grace Lewis says. That sounds obvious, but too many people fail to provide a basis for their claims, in Lewis's view.

In a small laboratory of computers running various environments, Lewis leads an SEI team performing TechCheck tests—"experiments to separate fact from fiction," Lewis calls them. The TechCheck approach is like the classic scientific method: set hypothesis, design test, and evaluate test results. In 2006, the TechCheck team reported results for tests of Web Services and the OWL Web Ontology Language for Services (OWL-S). Web Services has attracted interest in the U.S. Department of Defense and many other organizations. The OWL-S describes the properties and capabilities of Web Services so that a computer system can interpret them in an automated manner.

The TechCheck approach gives the SEI credibility. Striving for credibility is nothing new for Lewis. A desire to establish credibility is why Lewis earned a systems engineering degree in her adopted homeland of Colombia. It's why she later earned an MBA to be effective in an executive position, as chief of systems development for Universidad Icesi in Colombia. And it's why she left that position to pursue a Master of Software Engineering (MSE) degree from Carnegie Mellon University. Of her move between continents in search of the MSE: "I wanted to reestablish my technical credentials in order to contribute." Mentored by the MSE program director, Jim Tomayko, Lewis obtained her MSE and joined the SEI.

Lewis's team will next analyze the Open Grid Services Architecture (OGSA), the Web Service Modeling Ontology (WSMO), and security standards for Web services. The goal of OGSA is to integrate components that might be in different organizations or parts of the world into effective systems. Similar in purpose to OWL-S, WSMO can facilitate the automated discovery, combination, and invoking of services over the Web.

In addition to testing claims about technologies, Lewis and her team are working to transition the TechCheck approach from the laboratory to the field. They are designing workshops at which organizations can learn to assess the risks involved in filling the gaps between their business cases and the available technical capabilities.

In 2006, Lewis was invited to present the team's experiences at the inaugural Joint Integrated Air and Missile Defense Summit and the Semantic Technology Conference. "The SEI is increasingly seen as having something important to say in the area of emerging technologies," says Lewis.

Getting on the Right Track With Service-Oriented Architecture

Decades ago, Duke Ellington's signature song told audiences to "Take the A Train" and urged "Hurry, get on now." Today, organizations are hurrying to get on the *SOA* train. But Dennis Smith wants them to know where they're going and how long it will take to get there before they board.

The service-oriented architecture, or SOA, approach enables applications to be built from independent services that are accessed in a standard way. A key to successful development of an SOA is to make best use of legacy systems by recasting existing capabilities as services, which is a complex process.

For the past two years, Smith has led the SEI's effort to help organizations interested in adopting SOA approaches make informed, directed decisions that make good business sense and do not become regrets. Smith says, "The SEI has become a voice of sanity in helping organizations to sift through the claims about SOA approaches and has gained practical experience in what is real and what is hype."

Even as a still largely untested and rapidly evolving solution, an SOA approach can get organizations where they want to go if they are committed to following some basic principles the SEI has identified. These include "an understanding of how to align strategy with business goals, how to approach governance, how to analyze specific technologies, and how to migrate legacy assets to use as services within a specific SOA context," says Smith.

Smith, who holds a doctorate in sociology, took an unusual approach in his migration to a technology career. While working on a college's accreditation preparation, he discovered that numerous manual processes were choking the college's ability to provide services for students. He implemented an automated system and improved service delivery.

Sociologists will point out that their field, in its simplest terms, involves the study of two or more people *in a situation*. Smith's interest then, as now, is in the context in which technology happens. His approach to migrating legacy systems is not only in how to get data from one platform to another, but also in how a chosen solution meets the needs of people who will use it. Thus, the migration technique developed at the SEI begins: "Establish stakeholder context."

Smith leads an SEI team that aims to make the SEI an SOA center of excellence. In addition to writing articles on SOAs for publications such as *The DoD Software Tech News*, Smith's team developed a tutorial on SOA basics and techniques for migrating legacy assets to SOA, which Smith and Grace Lewis have delivered at conferences and customer organizations. Smith and Lewis are converting the tutorial into a public course that will be available in early 2007.

Smith and Lewis have also been instrumental in putting the SEI-developed Service-Oriented Migration and Reuse Technique (SMART) to use in the U.S. Army's Communications Electronics Research Development and Engineering Center. SMART enables an organization to understand what it needs and what it lacks in order to develop a sound legacy-system-migration strategy.

Smith and his team are helping organizations get on the right track to evaluate their legacy applications, evaluate the potential pitfalls, and make informed decisions about adopting SOA.

"The SEI has become a voice of sanity in helping organizations to sift through the claims about SOA approaches and has gained practical experience in what is real and what is hype."
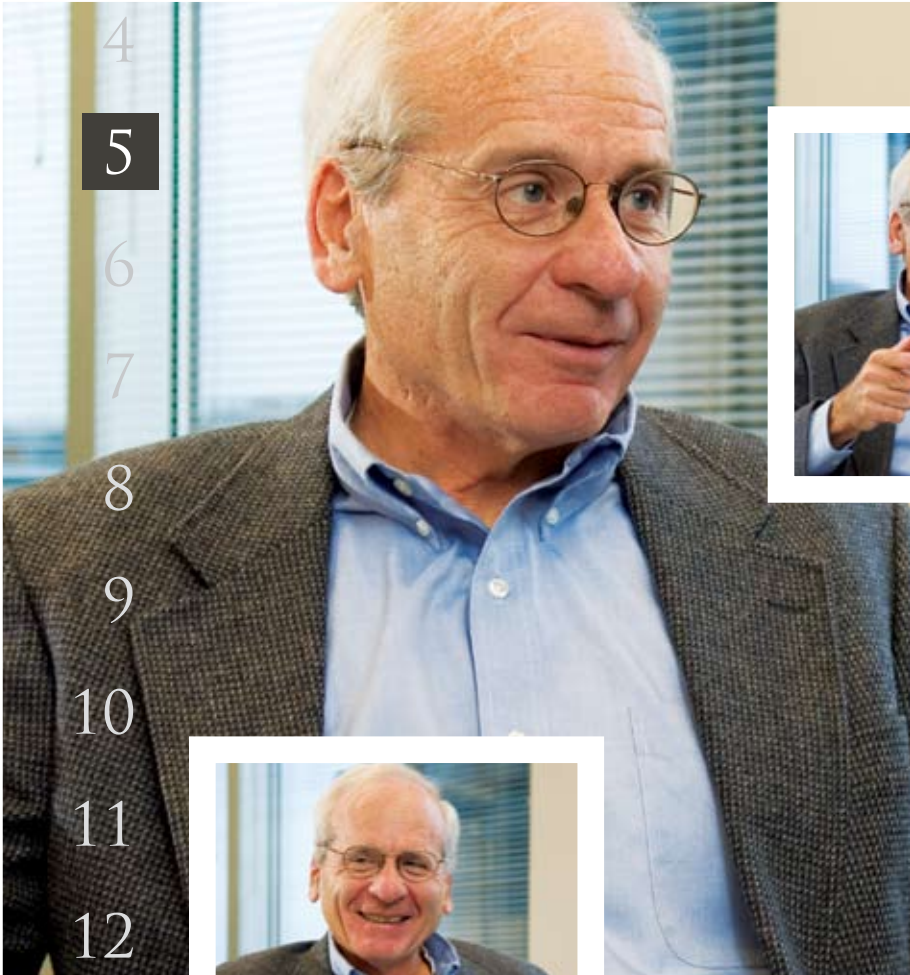

In addition to Dennis Smith, the SEI team working on SOAs includes Grace Lewis, Soumya Simanta, Lutz Wrage, and Ed Morris. The work on SOAs and the SMART migration approach relies on the extensive expertise developed by Lewis and other team members (see page 15).

DENNIS SMITH

> " There are a number of multinational companies establishing offices, factories, and software development centers in the region, and they are ready to understand process improvement for software-intensive systems. "

1

2

3

SUZANNE GARCIA AND GIAN WEMYSS

4

5

6

7

8

9

10

11

12

The growth of the SEI's influence in Latin America includes the increase in attendance at the Software Engineering Process Group Latin America conference during the past two years; the number of SEI Partners licensed to deliver services in Brazil, Chile, Colombia, and Mexico; and invitations to SEI staff members to present keynote speeches at Brazilian and Mexican conferences, such as the annual Software Guru conference. The SEI has also seen the number of CMMI appraisals grow in Argentina from 10 or fewer to 15 and in Brazil from 10 to 39.

13

14

15

16

SEI Exports Expertise to Latin America Where Technology Adoption Soars

Interest in SEI tools and methods among software-related industries in Latin America is increasing thanks in part to four individuals who are proud of their Hispanic backgrounds and experiences.

Suzanne Garcia, Grace Lewis, Philip Miller, and Gian Wemyss, who constitute the SEI team for the annual SEI and European Software Institute Software Engineering Process Group Latin America (SEPG[SM] LA) conference, have combined their personal connections with Latin America and their dedication to the SEI to help transition SEI technologies into a region that is emerging in the field of software engineering. Gartner Research reported in December 2005 that the Latin American growth rates for technology adoption, IT services, and outsourcing are among the highest in the world.

Lewis and Wemyss are of Colombian and Chilean descent respectively, while Garcia is connected to Latin American heritage through marriage. Miller has spent part of the past 13 summers in Mexico and Guatemala supporting two medical clinics, an orphanage, and a school.

When the team members begin talking about their professional and personal experiences, a central theme emerges: the importance of family and community. In a way, this team has formed its own family. Meetings and teleconferences are easy, quick, and engaging exchanges on work, family, and future SEI work in Latin America. Speech moves easily between Spanish and English.

"There are a number of multinational companies establishing offices, factories, and software development centers in the region, and they are ready to understand process improvement for software-intensive systems,"

Wemyss says. "But, just as important, there are a number of Latin American homegrown organizations that are beginning to understand the competitive advantage of process improvement."

Garcia agrees: "The financial and automotive industries growing in Brazil are both heavily software dependent. In Mexico, there is a government-sponsored economic initiative called Prosoft that is looking to promote Mexican software organizations and the disciplines, such as the CMMI® framework, that they are employing to become more competitive in the global marketplace."

In July 2006, the SEI officially launched a pilot SEI Team Software Process[SM] (TSP[SM]) initiative with Mexico's Tec de Monterrey University. The goal of the initiative is to train 20 to 50 students as well as two major industry organizations in the TSP method. Miller says, "The SEI strategy is to enable Mexico to make TSP its own by building the critical pool of thousands of TSP developers supported by Mexican instructors and coaches."

The team members have a passion for taking the world-class assets of Carnegie Mellon University and the SEI to Latin American software organizations. Lewis believes that the team's use of Spanish, its varying multicultural experiences, and its commitment to its work enable the SEI to move technologies into a large enough market that there is an easy, visible benefit.

Perhaps Miller says it best: "I am a believer in using education for social mobility at the personal level and at the national level. It makes sense to me to put those two things together."

FCS Aims to Modernize the World's Most Capable Army

18 + 1 + 1: These numbers probably don't mean much to the average citizen, but for the Future Combat Systems (FCS) program, this formula sums up the U.S. Army's vision for the future. Developing and integrating 18 manned and unmanned systems, one network, and each soldier, FCS is one of the most complex undertakings ever attempted by the U.S. Department of Defense. Pair this level of complexity with the fluid nature of technology and, suddenly, just keeping track of all the variables becomes a massive endeavor.

Stephen Blanchette, Jr., the technical lead for the SEI's work with FCS, is accustomed to negotiating variables. He's spent the past two decades working on Army systems as a senior engineer, lead engineer, and program manager, all the while honing the communication and negotiation skills that now help him to reconcile the often disparate perspectives among stakeholders and customers. Holding a master's degree in diplomacy certainly helps. Blanchette says: "Studying diplomacy has helped me recognize that different people have different approaches. It's important to work together to find common ground."

Blanchette's knack for finding common ground, coupled with his broad technical background, has made him an asset to numerous government and defense organizations throughout his career. His dossier is stuffed with achievements; perhaps the most notable was receiving the U.S. Army Achievement Medal for Civilian Service for his work on the Bradley series of fighting vehicles.

The FCS modernization effort marks a fundamental change in how the Army will fight in the future and promises to significantly transform all aspects of battle and employ revolutionary operational and organizational concepts. This year, FCS achieved a significant milestone: in-process preliminary design review.

Meeting this milestone signifies that FCS is ready to move from systems definition to the hardware and software design and test phases. It also confirms that FCS is on track to meet cost, schedule, and performance projections.

Blanchette's collaboration with FCS focuses on the integration of all components into a family of systems. He works with the program's lead system integrator (LSI) to integrate the FCS family of systems. He leads a team of SEI experts who work with several of the LSI's teams such as the Software Analysis and Integration Team and the Information Assurance Working Group, which handles network security and survivability, among other concerns. In each of these areas, Blanchette leverages the expertise of almost every technical program within the SEI, and his enthusiasm is apparent: "The breadth of our experience helps customers identify and work through problems. Our broad perspective helps us to present the alternative solutions."

To Blanchette, FCS isn't just about building a network of systems. It is about building a network of people. Through their hard work, the world's most capable army will become more efficient, deployable, sustainable, and virtually unparalleled.

1

2 "Studying diplomacy has helped me recognize
that different people have different approaches.
It's important to work together to find
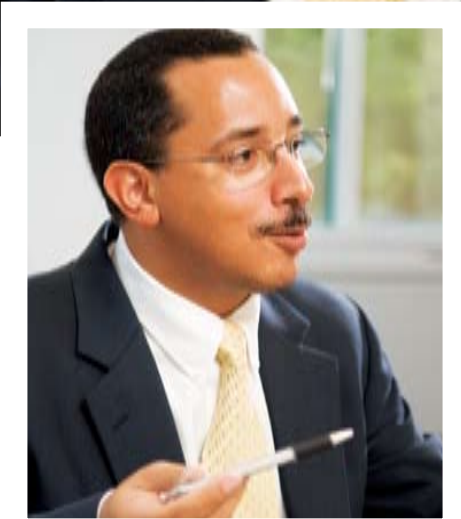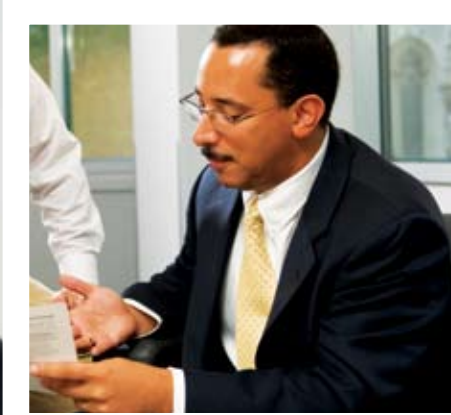3 common ground. "

4

5

6

7

8

9

10

11

12

STEPHEN BLANCHETTE, JR.

13

14

15

16

NANCY MEAD

Most software companies take the Band-Aid approach to security: They patch security flaws well after the software's public release and make firewalls and intrusion-detection software a necessity for safe Internet access.

https://buildsecurityin.us-cert.gov/

SEI Supports DHS Initiative to Build Security In From the Start

Most software companies take the Band-Aid approach to security: They patch security flaws well after the software's public release and make firewalls and intrusion-detection software a necessity for safe Internet access. But Nancy Mead of the SEI wants to revolutionize how software is developed so that security is no longer an afterthought.

As the technical lead of the Build Security In (BSI) Software Assurance Initiative, Mead promotes software design that is less vulnerable to attack. "BSI's primary objective is to provide software developers and managers with advice, examples, and methods for developing more secure software from the start rather than only using patches and firewalls to treat the symptoms of vulnerable software," she says.

BSI is a project of the National Cyber Security Division (NCSD) of the U.S. Department of Homeland Security. NCSD has sponsored the development and collection of software-assurance and software-security information that will help software developers and architects create secure systems.

Last year, BSI launched a collaborative Web site that encourages security researchers and professionals to publish and discuss security engineering research. "The site's goal," Mead says, "is to increase the body of knowledge in secure software engineering." In addition to contributing her own content in the areas of requirements engineering and business cases, Mead determines gaps in the site's content, solicits new research, and reviews submitted papers. The result is a comprehensive site for researchers, developers, and executives.

One of the threads that runs throughout Mead's long career is education. She has been, at various times, a researcher, developer, and manager, but always a teacher. She combined her early focus on requirements engineering, which stems from her position at IBM as a large-scale software architect, with her role as course developer—she eventually headed up the education function in IBM's Federal Systems Division. Spaces filled quickly in her classes. Developing the curriculum opened her eyes to the requirements research yet to be done. When she came to the SEI, Mead continued her research and teaching, focusing on the relationship between requirements engineering and security. At the SEI, she developed the SEI Security Quality Requirements Engineering (SQUARE) methodology for eliciting and prioritizing security requirements in software development projects.

Part of the BSI initiative includes publishing an online content catalog, which contains or links to a broad range of information about best practices, tools, guidelines, rules, principles, and other knowledge to help organizations build secure and reliable software.

Mead, who also is an adjunct faculty member at Carnegie Mellon University and a fellow of the Institute of Electrical and Electronics Engineers (IEEE), has high hopes that the BSI Web site will encourage developers to take a new approach to software security. "Education is the way to get at the root of a problem," she says.

By Tracking Value Creation in Cyberspace, SEI Aims to Stay a Step Ahead of the Bad Guys

Tom Longstaff spends a lot of time reading RSS feeds from BoingBoing.net, a self-billed "directory of wonderful things" ranging from technological to political to just plain zany.

It's not that the site has direct relevance to Longstaff's job as head of research for the SEI's Networked Systems Survivability Program. Rather, "it has relevance for where security is going," he says. "You have to understand where the value is being represented in cyberspace. It's not a constant. It shifts all the time. You have to stay close enough to see where a trend begins to catch on."

Where there is value, there will be attackers who want to steal or destroy that value. The best defense is to know where the value will be, before the attackers can act. "If you just watch the bad guys," Longstaff says, "you're one step behind."

Longstaff was born in Unity, Maine, the eldest son of the town minister. His first brush with computer security came in the early 1980s, while he was studying for his PhD in applied science at Lawrence Livermore National Laboratory. His Sun 2 workstation was attacked over the ARPANET, the precursor to the Internet. "The security group at Livermore Lab and the intruder were fighting it out on my machine. I was so fascinated that it changed the whole course of my career. I saw computer security as the place to be."

He joined Livermore's computer incident advisory team and wrote several papers on malicious computer code, worms, and viruses, building a reputation among incident-response researchers and practitioners.

In 1991, the SEI recruited Longstaff to lead a new research area in computer security.

Today, Longstaff and others at the SEI study ways to simplify security to make it much less time-consuming and burdensome. In a 2006 research project, he and principal investigator Gwen Walton posed the question, "What can be computed with respect to security attributes of software?" They determined that security properties can in fact be evaluated through computational automation and can also be specified—a major shift away from current approaches that assume that security is a nonfunctional attribute.

"Most software follows a few simple rules and can be specified. If all the security happens in the areas you can specify, then the security can be specified by its actual behavior," Longstaff says. "The idea is to make all the behavior related to security in software immediately visible, so you're no longer talking in the abstract, but specifically about how the software behaves to support security. It sounds simple, but it's a complete redefinition of the way we describe security attributes for programs."

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16

TOM LONGSTAFF

" You have to understand where the value is being represented in cyberspace. It's not a constant. It shifts all the time. You have to stay close enough to see where a trend begins to catch on. "
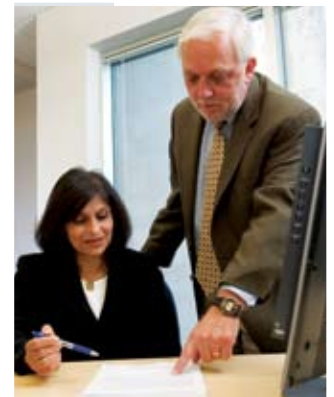
1
2
3

4
5
6
7
8
9
10
11
12

Jim Over

13

"The SEI is all about getting people to use the best practices, tools, and methods. Our focus is on practical application."

14
15
16

NAVAIR Extends TSP Methodology to Systems Engineering and Acquisition

"The SEI is all about getting people to use the best practices, tools, and methods," says Anita Carleton of the SEI technical staff. "Our focus is on practical application."

To that end, Carleton and her colleagues on the SEI Team Software Process (TSP) team work with personnel at the U.S. Naval Air Systems Command (NAVAIR) to institutionalize the TSP methodology within NAVAIR. In FY 2006, the SEI and NAVAIR began a project to extend the use of TSP from software development to systems engineering and acquisition management.

NAVAIR, which develops, acquires, and supports the aircraft and related weapons systems used by the U.S. Navy and Marine Corps, was one of the first organizations to adopt TSP for improving its software development practices—others include Intuit, Microsoft, and Oracle. TSP has not only accelerated process improvement efforts at NAVAIR but has also led to a cost savings of $1.5 million to $2 million on several projects. In light of these results, it is natural for NAVAIR now to consider applying TSP practices more broadly.

Carleton's enthusiasm for TSP is rooted in her experiences as a software developer in industry in the 1980s. "I struggled with software issues that the SEI was then just beginning to identify," she says. "During the early days of the SEI Process Program, when I interviewed with Watts Humphrey, I was excited to learn that the mission of the program aligned closely with my interests in applying quantitative methods for improving software development processes."

A college mathematics major with a primary interest in software measurement, Carleton had always wondered why software developers lacked quantitative data on which to base decisions. At the SEI, she worked with Humphrey, an SEI fellow, who managed the Process Program at that time, and helped to define core measures for software development that later formed the basis of government policy for software development and acquisition. Concentrating now on TSP, says Carleton, is "a logical next step because TSP shows engineers exactly how to apply measurement practices. So I'm doing the work I always wanted to do."

TSP team leader Jim Over is equally passionate about measurement and the benefits realized from the practical application of TSP. "In trying to do process improvement before," he says, "you could talk to managers, but engineers would still work the same way they always did. TSP-trained engineers now have the tools to actually put improvement ideas into practice."

Humphrey, Carleton, Over, SEI colleague Noopur Davis, and the NAVAIR team—Tim Chick, Dennis Linck, Linda Roush, Jeff Schwalb, and Paula Strawser—are conducting a series of pilot projects to determine if extending TSP practices to systems engineering and acquisition management results in measurable improvement. "The whole team is dedicated to making this all work for NAVAIR," Carleton says.

By dissecting malware, the artifact analysis team is compiling a wealth of information about malware and those who use it.

Rob Murawski

KEVIN HOULE

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
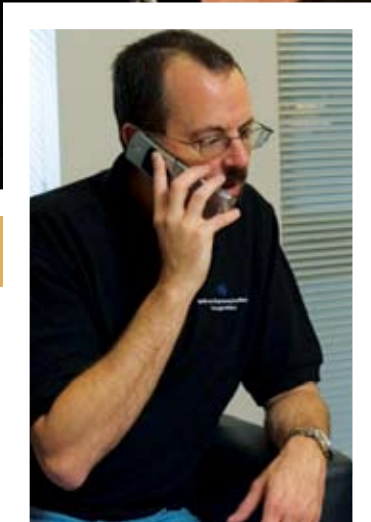
Understanding Botnets

Nick Ianelli's years as an ISP technical support manager and network and systems engineer gave him valuable experience in tracking down network abusers. Currently, Ianelli is focused on botnets—compromised computers under the control of an attacker. Attackers use botnets for a variety of criminal activities. "Botnets are a huge problem for many of the communities we interact with," notes Ianelli.

He and fellow analyst Aaron Hackworth analyzed botnet malware and detailed their findings in *Botnets as a Vehicle for Online Crime*, a paper adopted by Interpol and distributed to its 186 member countries.

Researchers Probe Activity of Online Criminals by Dissecting the Tools of Their Trade

Kevin Houle's artifact analysis team confronts the realities of today's networked world, a world in which criminals and others target financial and informational assets. These attackers leave behind artifacts in the form of malicious computer code, or "malware." By dissecting malware, the artifact analysis team is compiling a wealth of information about malware and those who use it, while at the same time creating a new discipline in the fields of computer security and law enforcement.

"Our research produces insight on how technology fails, what assets adversaries target, how they acquire targets, who the adversary is, and how we can raise awareness about malicious code," says Houle. "We provide an analysis capability, encourage the adoption of analysis techniques and tools, and foster advancement of the practice among law enforcement, technologists, asset holders, and other interested communities."

The artifact analysis team's work extends beyond research. "We provide our collaborators and sponsors the tools and education needed to streamline analysis and more quickly answer specific questions," says analyst Nick Ianelli. The team also worked closely with federal law enforcement to shut down and apprehend a major identity theft and fraud ring whose activities inflicted more than $4 million in losses.

Houle's tenure as manager of networking and systems for a regional Internet service provider (ISP) prepared him for the work he leads today. "That rapid-change environment gave me insight about how the Internet functions and who the key players in Internet infrastructure are."

Analyst Rob Murawski found that an inquisitive nature and background in programming and computer hardware prepared him for his work at the SEI.

"As a programmer," says Murawski, "I was intrigued by tearing things apart to see how they work."

Murawksi's current research centers on data exfiltration: the methods, tools, and technologies attackers use to steal data assets (passwords, account numbers, sensitive corporate data) from networked systems and slip those assets past system and network defenses. "Data exfiltration capability is ubiquitous in malware," notes Murawski. "That makes analysis difficult."

Recently, Murawski reported his findings in the paper *Data Exfiltration Techniques: How Attackers Steal Your Sensitive Data.* Murawski notes that attackers tend to use just enough technology to achieve their aims. However, when necessary, they can craft sophisticated exfiltration techniques. For instance, one malware sample exfiltrated stolen data by inserting it in normal-looking ping packets, which are not typically monitored by network-defense tools.

"There's definitely an element of detective work in what we do," notes Murawski. "You not only have to be a good solver of puzzles, you have to have the ability to recognize the puzzles in the first place and enjoy attacking them from different angles."

Ianelli picks up the thought: "Artifact analysis isn't something you go to school for—yet. We're developing the field as we perform and refine our analyses." Summing up his team's strengths, Houle observes, "Our team possesses what I think are the essential characteristics for success: a belief in and passion about our mission, self-motivation, a drive to constantly learn and improve, and a deep technical foundation in Internet and software technologies."

JILL DIORIO

"The role of the SEI is to be an objective broker for our clients. Avoiding conflicts of interest and preserving confidentiality have always been very high priorities."

SEI Institutes Control Board and Hotline Program to Support Compliance Activities

In a way, formalizing a code of professional conduct was natural for the SEI, given what the institute specializes in. "We're all about methods for establishing quality, compliance to process, and information security," states Jill Diorio, manager of the SEI Partner Network Ethics and Compliance Program.

"The role of the SEI is to be an objective broker for our clients," explains Diorio. "Avoiding conflicts of interest and preserving confidentiality have always been very high priorities."

Diorio is working to expand the ethics and compliance program based on the SEI's existing Code of Professional Conduct (CoPC). In May 2006, she established the CoPC Review Board in collaboration with SEI colleagues and SEI-licensed partners—organizations and individuals authorized to deliver SEI methods, courses, and processes. For example, licensed partners often provide assessments of customer practices based on SEI models. It's crucial that these assessments be objective and verifiable and that no conflicts of interest arise.

The partners nominated and elected a board composed of well-respected peers, whose main function is to provide, on request, independent reviews of data gathered and investigative findings regarding possible noncompliance. Diorio believes that a review board comprising members who are elected representatives from the community will ensure fairness, inclusiveness, and objectivity.

The Ethics and Compliance Hotline, instituted in August 2006, was established to provide a channel for reporting ethics and quality-compromising issues anonymously. "We have always encouraged open dialogue; individuals should feel free to contact the Compliance Program or any SEI staff member for guidance or to discuss concerns," states Diorio.

"But we also recognize that circumstances may necessitate the option to report a matter anonymously."

Web-based training on ethics and compliance, another of Diorio's proposed initiatives, is in development. It will address the everyday situations that SEI Partners may encounter when delivering SEI-licensed products. New and timely topics will be rolled out regularly.

While Diorio supports federal laws now controlling accountability for corporations and privacy for consumers, she strongly believes that organizations, employees, and management must be proactive in the development and execution of ethics and compliance programs. This is crucial to demonstrating the organization's commitment to ethical behavior and to carrying this commitment into all its business activities and overall mission. "Being proactive means developing a code of conduct in accordance with your specific organizational needs; this promotes both acceptance and ease of adherence to the code," she says.

Diorio concludes simply, "Compliance must be built into the culture. Fortunately that has always been the case at the SEI."

As software engineering matures even further, so will the need to develop an expanded and refined conduct code for its professionals. The SEI will be on the forefront of future developments.

SEI Develops Cyber-Forensics Platform for DHS

Rich Nolan talks a lot about scalability, and talking to him is to experience things on a large scale. A burly Marine Corps veteran with an imposing voice who still sports a military-style haircut more than a decade after his active duty, he has big goals and big ideas. For example, he wants to use the ReFORCE platform to improve the U.S. government's computer forensics capability.

ReFORCE is the Remote Forensics Computing Environment, which was developed in 2006 by Nolan, Matthew Geiger, and Cal Waits from the SEI and sponsored by the U.S. Department of Homeland Security (DHS). ReFORCE is a computer forensic analysis platform that is remotely available to federal, state, and local authorities. The robust environment includes new research and analysis techniques developed by the SEI. But what capability does ReFORCE improve?

Nolan, who as a Marine, was stationed in the Balkans during the Bosnian crisis and later served as a Drug Enforcement Administration (DEA) agent for seven years, explains the genesis of the idea: As a DEA agent, he worked on a nationwide case relating to the Internet sale of illegal drug paraphernalia. Investigators executed nearly 60 concurrent search warrants and seized hundreds of computers, but the turnaround time for forensic analysis would be long. Valuable leads about the money trail might come too late.

The typical model then, as now, was for each agency to set up its own small forensics lab—replicating hardware, software, and training, and limiting each lab's resources. ReFORCE is a scalable platform that can be securely shared by DHS, law enforcement, and other agencies.

The new platform, says Nolan, can be scaled up to meet DHS needs during a crisis, or parts of it can be used independently by other authorities during down times. The ReFORCE platform is more powerful and cost-effective than any other option currently available to investigators and analysts.

Nolan, who can change from boisterous to self-effacing in an instant, deflects praise and credits his fellow team members Geiger and Waits for their roles in the development and testing of ReFORCE. Both Geiger and Waits began working with Nolan when they were graduate students in the Carnegie Mellon School of Computer Science. Before coming to Carnegie Mellon, Geiger spent 14 years in Southeast Asia as a foreign correspondent for Dow Jones, a financial analyst who helped develop the first online banking operation in Malaysia, and the founder of a computer forensics company in Singapore. Waits is a former philosophy student, missionary, and National Security Agency (NSA) computer forensics specialist.

"Although we have a rich technical knowledge, that isn't the most important thing," says Nolan about his team's varied backgrounds. "Having a broad-based ability to learn is far more valuable."

The ReFORCE platform is more powerful and cost-effective than any other option currently available to investigators and analysts.
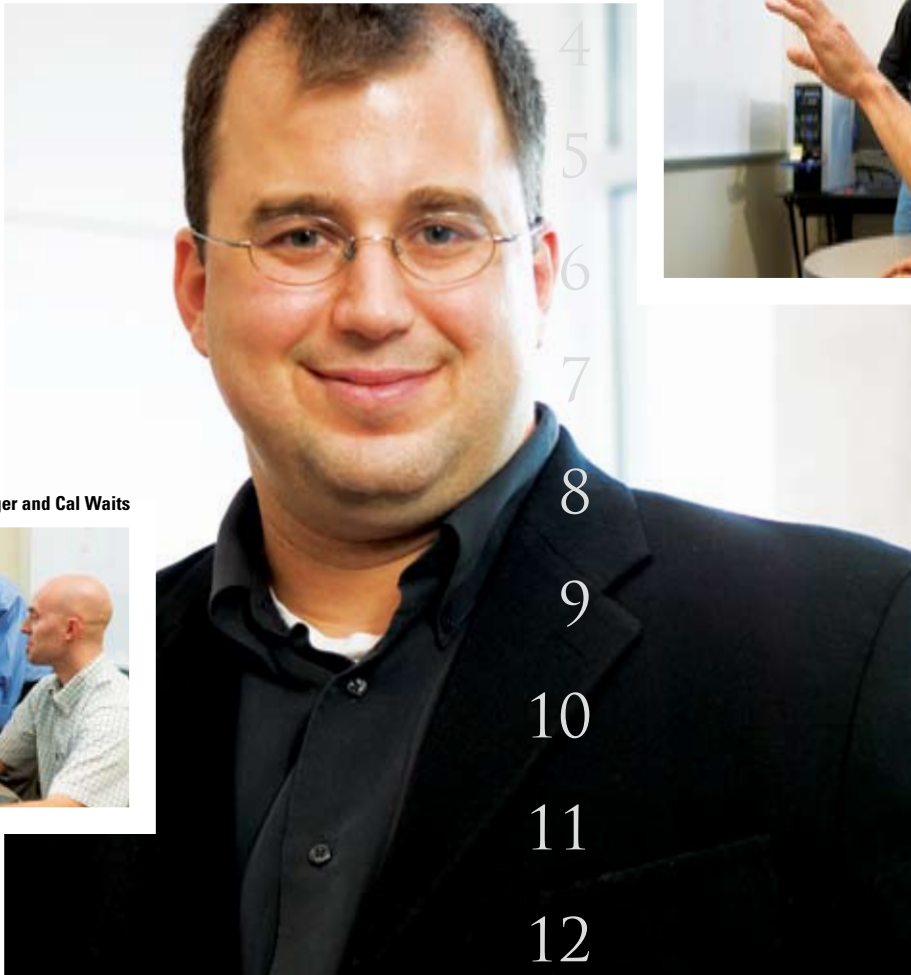
1

2

3

4

5

6

7

8

Matthew Geiger and Cal Waits

9

10

11

12

RICH NOLAN

13

14

15

16

What Is Computer Forensics?

The Department of Homeland Security's US-CERT defines computer forensics as "the discipline that combines elements of law and computer science to collect and analyze data . . . in a way that is admissible in a court of law." If organizations ignore computer forensics techniques or practice them badly, they risk destroying vital evidence or having it ruled inadmissible. The application of computer forensics is obvious in cases of Internet fraud, cyber threats, or network intrusions, but these are not the only crimes where computer forensics comes into play. "Almost any type of crime may have a computer dimension," says Rich Nolan of the SEI, who co-wrote a handbook on computer forensics. "Suspects may have sent emails, conducted online chats, or downloaded material from the Internet; this information can be used to build a case against them in court."

Mary Ann Lapham

Mary Ann Lapham leads the SEI team that is providing support to the Transformational Satellite Communications (TSAT) program, which is working to develop the next generation of secure communication satellites. Like the Space Radar program, TSAT relies heavily on software. Lapham has more than 30 years of experience in all areas of computer software and systems engineering as well as project and people management. Since starting at the SEI, Lapham has been devoted to "raising programs' awareness of problems in unprecedented software-intensive systems" by helping them understand the many issues surrounding large-scale software integration.

For the TSAT program, Lapham and her team are advising on architecture, development, and integration and consulting on system and network engineering and integration solutions. Her biggest challenges to date have been imparting the importance of seamless software integration and the necessity of successfully managing the software acquisition life cycle.

1
2
3

TED MARZ

4
5
6
7
8
9
10
11
12
13

14 "The experience and knowledge I gain from being embedded in a management position in the program office is what I'll eventually bring back to improve the acquisition program of the SEI."

15
16

SEI Veteran Leads Software Effort for Advanced Radar Program

The day's rhythm is different now for Ted Marz. Each day starts with a brief stand-up meeting at which the day's priorities are set; his daily activities include not only technical work, but also work on budgets, resources, and schedules now that he is a manager in the Space Radar program.

Marz, a senior member of the technical staff at the SEI, was asked to lead the software division for Space Radar, a joint venture of the U.S. Department of Defense (DoD), intelligence services, and civil agencies. As software division chief, Marz is essentially on loan from the SEI through an Intergovernmental Personnel Act (IPA) assignment with Space Radar.

Since joining the SEI, Marz has worked on improving software acquisition processes for the DoD. His experiences within the SEI and elsewhere have given him a sound foundation in technology research and development that he can use in his new technical leadership role with the Space Radar program.

Space Radar will use multifunctional radar to support real-time tracking of surface targets for the DoD, intelligence services, and civil agencies. Space Radar will consist of many satellites and ground-control components that tightly integrate with intelligence systems, making Space Radar a complex software-intensive system of systems comprising millions of lines of code. It will implement more functionality than ever using software; this is why the Air Force turned to the SEI for help in assuring success and why the SEI turned to Marz.

"I'm a strong believer in trying to do things the right way," he says.

For Marz, the challenges of leadership are as complex as the systems themselves. As software division chief, Marz is leading a team that is working on developing and validating a system requirement set to satisfy a diverse group of stakeholders.

Currently, Marz is developing risk-reduction strategies for software acquisition as well as defining software strategies. Marz sees this assignment as an opportunity to apply industrywide best practices to new types of problems.

"The experience and knowledge I gain from being embedded in a management position in the program office is what I'll eventually bring back to improve the acquisition program of the SEI," he says.

CMMI Product Suite Looks to the Stars in Version 1.2

The initial move toward the next generation, Version 1.2, of the Capability Maturity Model® Integration (CMMI®) Product Suite took place in August 2006 with the release of CMMI for Development. The revised material employs a new architecture and a new term—*constellations*—to describe how components are grouped. That description should not come as a surprise to anyone who knows Roger Bate, chief architect of the CMMI Project.

But first things first. CMMI is a process improvement approach that provides organizations with the essential elements of effective processes. CMMI has provided a way for organizations to evaluate and describe the quality of their software and systems engineering development and maintenance processes. But what if an organization that has experienced the benefits of using CMMI for development wanted to use CMMI to analyze its acquisition practices? The CMMI Steering Group decided that a new architecture would help CMMI expand its coverage and extend into other domains.

Bate gave some thought to future needs of CMMI users and how the architecture could meet those needs. "I thought of CMMI's collections of best practices as the stars of process improvement," he says, "and I pushed the metaphor a little further to call a collection of model, training, and appraisal components for an area of interest a constellation." The metaphor came naturally to Bate, now in his 80s, an SEI fellow, Rhodes scholar, and the first chairman of the Astronautics Department at the U.S. Air Force Academy.

Bate's interest in process improvement started in the late 1970s when he was leading the Advanced Software Technology Department at Texas Instruments and was tasked to solve "the software problem." This phrase was used in the defense industry to describe the problems that project managers would cite when trying to explain why their projects were over budget or late. Working with Edith Martin, who was the deputy under secretary of defense for research and advanced technology, and Larry Druffel, who was the director of computer systems and software in Martin's office, Bate organized a workshop that brought together 300 experts to study the issue. The result of that workshop was the idea for the Software Engineering Institute. Druffel would later become SEI director.

CMMI for Development is the first of three constellations defined in Version 1.2. The other two constellations, to be released in 2007, are currently under development: CMMI for Acquisition and CMMI for Services.

The CMMI Steering Group expects Bate's new architecture to have important implications: It establishes the CMMI framework in a position of agility, adaptability, and extensibility for future development.

The revised material employs a new architecture and a new term—*constellations*—to describe how components are grouped.
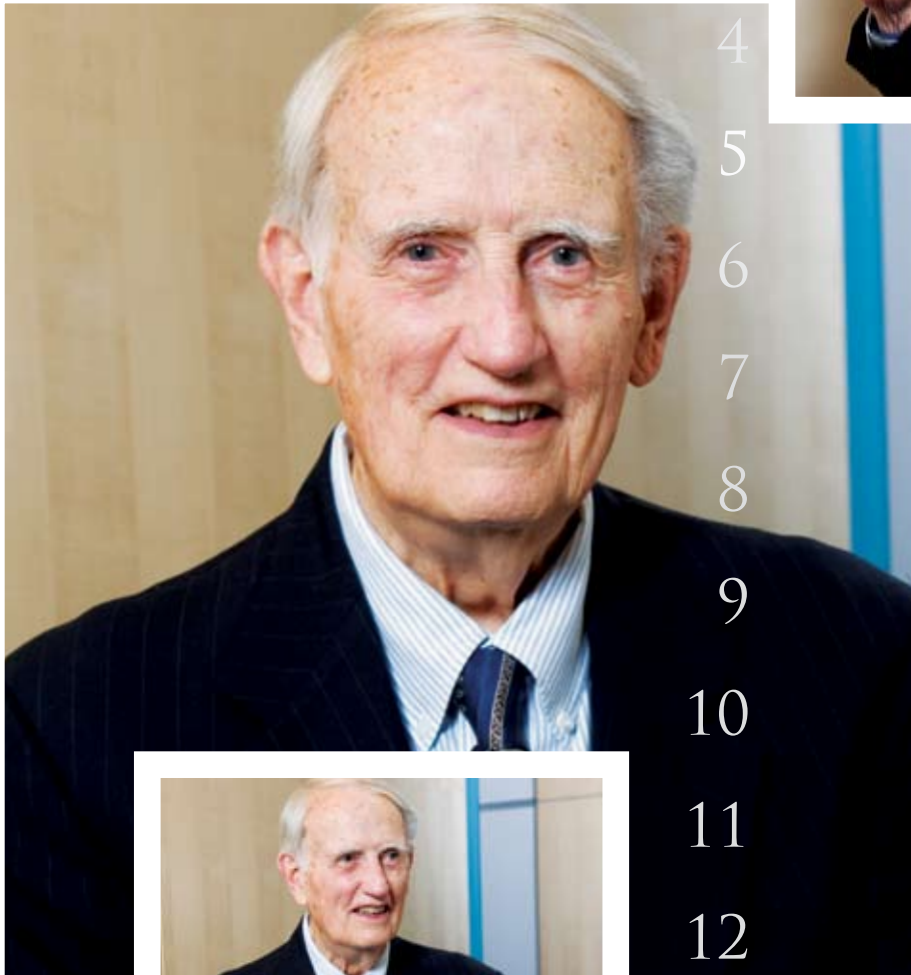
ROGER BATE

CMMI Project

The CMMI Project, formed in 1998, includes team members from government, industry, and the SEI. The three primary groups that compose the CMMI Project are the Steering Group, Product Team, and Configuration Control Board.

The Steering Group, co-led by Bob Rassa of Raytheon and Mike Nicol of the U.S. Air Force, guides and approves the plans of the Product Team, provides leadership on significant CMMI project issues, and ensures involvement from a variety of interested communities.

The Product Team, led by CMMI project manager Mike Phillips of the SEI, writes, reviews, revises, discusses, and agrees on the structure and technical content of the CMMI Product Suite, including the framework, models, training, and appraisal materials. Development activities are based on guidance from the Steering Group, source models, change requests received from CMMI users, and input received from pilots and stakeholders.

The Configuration Control Board, led by Mike Konrad of the SEI, is the official mechanism for controlling changes to the CMMI models, Introduction to CMMI training, and the Standard CMMI Appraisal Method for Process Improvement (SCAMPI^{SM}) methodology. As such, this group ensures integrity over the life of the product suite by reviewing and approving changes to the baseline.

JEFFERSON WELCH

The recent creation of international standards for certification programs by the International Organization for Standardization (ISO) and American National Standards Institute (ANSI) is highlighting the importance that certifications have in a profession that is quickly developing some of the most important tools for protecting human safety.

" We're recognizing the need for certification programs for the professionals who are responsible for the software and systems that drive [vital] industries. Public safety now depends on it. "

Certifications for Professionals in Software Engineering Help Assure Safety of Vital Systems

As a former aviation training professional, Jefferson Welch knows firsthand the importance of standard practices for professionals. "The aviation industry has a long history of ensuring safety through training, certification, recertification, and continuing education. This kind of training is becoming a necessity for professionals in the software industry. As software becomes vital to some of our most important activities, competence in the practice ensures the safety of our systems," Welch explains.

For almost 17 years, Welch trained pilots; at one time, he supervised more than 30 instructors responsible for training 5,000 pilots. "In aviation, pilots enter a lifetime of training, checking, and continuing education. This philosophy assures us that they are competent to enter and grow in the field. It's an approach that ensures public safety," he explains.

When Welch accepted his current position as manager of SEI Certification in 2004, he saw an opportunity to apply this approach to certification in software engineering. His first project at the SEI was a revision to the CERT®-Certified Computer Security Incident Handler (CSIH) program, the SEI's only certification program at the time. Welch is now leading an effort to have this certification join other certifications for information assurance professionals in the U.S. Department of Defense (DoD). With the passage of DoD Directive 8570 in 2005, all DoD information assurance employees must earn and maintain one of several DoD-approved certifications. "We are planning to seek ANSI 17024 accreditation for the CERT-Certified CSIH program in order to be listed as fulfilling the requirements of DoD 8570," says Welch, who expects to complete this effort in early 2008.

Following his work on the CSIH certification, Welch helped to introduce three new SEI certifications: SEI-Certified PSP* Developer, SEI-Certified Implementing Goal-Driven Measurement Instructor, and most recently the SEI-Certified SCAMPI High-Maturity Lead Appraiser. Since the PSP Developer certification was released at the SEI's March 2006 Software Engineering Process Group conference, more than 55 professionals have earned PSP Developer certification.

Participation from software engineers and software engineering organizations confirms the importance of PSP certification. During the development of the PSP Developer certification, the PSP Body of Knowledge—the document that is the basis for the questions on the PSP Developer examination—received more than 100 reviews from professionals who have applied PSP to their work. Welch and his colleagues on the SEI Certification team continue to rely on participation from government, industry, and academia as they develop new certification programs. Certifications in progress include TSP Coach, SCAMPI Lead Appraiser^{SM}, PSP Instructor, and Software Architecture Principles and Practices Instructor certification.

"Establishing standards for the practitioners is a necessary step as a profession matures," says Welch. "As we depend more on software and systems engineering in health care, transportation, security, and law enforcement, we're recognizing the need for certification programs for the professionals who are responsible for the software and systems that drive those industries. Public safety now depends on it."

*Personal Software Process^{SM} methodology

Outreach

SEI Partner Network

The SEI Partner Network consists of organizations and individuals trained and authorized or certified by the SEI to deliver official SEI services worldwide. These services include courses, consulting methods, and management processes that aid in the implementation of the SEI's software engineering technologies. Partners who deliver SEI services are trained and evaluated by the SEI to ensure that they have the necessary knowledge and skills. In FY 2006, the SEI Partner Network consisted of 554 license agreements, 310 partner organizations, and 1,654 authorized and certified individuals. The online SEI Partner directory extends the availability of SEI services delivered through partner organizations by making SEI Partner information readily available to those seeking training in SEI methods, processes, and technologies.
www.sei.cmu.edu/partners

SEI Membership

SEI Membership fosters the relationship between the SEI and the software engineering community. In FY 2006, the program had more than 2,000 members worldwide. Members are leaders in software engineering and include CEOs, directors, and managers from government, business, industry, and academic organizations. The program provides software engineering leaders priority access to SEI technologies and events that support the transition of standards and best practices. SEI Membership provides members with many opportunities to advance, network, and learn through collaboration with the SEI and each other. Many members have used their SEI memberships to increase their professional standing and affiliations.
www.sei.cmu.edu/membership

SEI Conferences and Events

The SEI sponsors and co-sponsors many conferences, workshops, and user-group meetings. These events represent technical work and research in the areas of process improvement, software architecture and product lines, security, acquisition, dependability, and interoperability of systems. The SEI serves as host of the quarterly U.S. Army Senior Leader Education Program, which 125 individuals have attended. In FY 2006, SEI events drew nearly 4,000 attendees from around the world. SEI-sponsored or -cosponsored signature events include the U.S. and international Software Engineering Process Group conferences, Software Product Line Conference, Workshop on Flow Analysis (FloCon®), International Conference on COTS-Based Software Systems (ICCBSS), and the International Process Research Consortium.
www.sei.cmu.edu/events

SEI Education and Training

SEI Education and Training helps bring SEI technologies and best practices into widespread use. In 2006, the SEI offered 290 courses in process improvement, information security, software architecture, software product lines, acquisition management, organizational management development, and model-based engineering. In FY 2006, the SEI trained 5,653 individuals from government, academia, and industry, while SEI Partners trained 15,598 individuals for a total of 21,251.
www.sei.cmu.edu/products/courses

SEI Affiliate Program

Through the SEI Affiliate Program, organizations place technical experts with the SEI for periods ranging from six months to four years. In FY 2006, 28 affiliates were working on projects with the SEI to identify, develop, and demonstrate improved software engineering practices.
www.sei.cmu.edu/collaborating/affiliates

Leadership, Management, & Staff

SEI Director's Office

The SEI Director's Office ensures the smooth, efficient operation of the SEI. Director and CEO Paul Nielsen and Chief Operating Officer Clyde Chittister build strong, collaborative relationships with leaders in government, industry, and academia, communicating the SEI's vision for software engineering.

Paul D. Nielsen is the director and chief executive officer of the SEI. Before joining the SEI in 2004, he served in the U.S. Air Force, retiring as a major general after 32 years of distinguished service in various jobs at headquarters level and in the field. Most recently, he served as commander of the Air Force Research Laboratory, Wright-Patterson Air Force Base, Ohio, where he managed the Air Force's science and technology budget of more than $3 billion annually.

Clyde G. Chittister is the chief operating officer of the SEI. He joined the SEI in 1985 and has held several senior management positions. He initiated and managed the Ada-Based Software Engineering Program, the Systems Program, and the Software Risk Management Program. He also managed the Industry Sector, which focused on establishing and building relationships between the SEI and industry clients.

SEI Management Team

The SEI management team leads the SEI by setting and executing SEI strategies, goals, and priorities and demonstrating the SEI core values of impact, excellence, and integrity.

Sally Cunningham
Director, Technology Transition Services

Patricia Oberndorf
Director, Dynamic Systems

Terry Dailey
Acting Director, Program Integration

Brian Gallagher
Director, Acquisition Support

William Peterson
*Director, Software Engineering
Process Management*

David Thompson
Director, Information Technology

Linda Northrop
Director, Product Line Systems

Jerry Bosken
Director, Administration

Richard Pethia
*Director, Networked Systems
Survivability*

Peter Menniti
*Director, Financial and
Business Services*

SEI Staff

The SEI attracts top talent to implement its expanding objectives, increasing its staff by a third over the past four years. Staff members are permanent, full-time employees; affiliates are professionals sponsored by their home organizations to work on SEI technical projects; visiting scientists are temporary SEI employees from government, industry, and academia.

Previous Affiliation of Visiting Scientists

Industry **52%**

Academia (CMU) **12%**

Academia (non-CMU) **11%**

Government **25%**
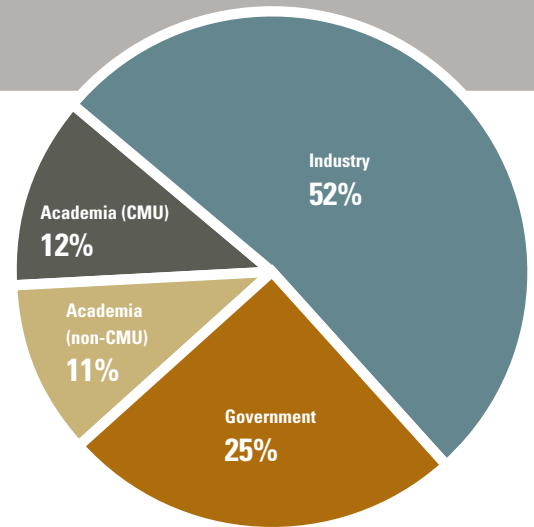
Technical and Operational Staff Academic Degrees and Experience

18% have a PhD, with an average of 32 years of experience

43% have a master's degree, with an average of 24 years of experience

32% have a bachelor's degree, with an average of 16 years of experience

310 technical and operational staff

128 visiting scientists

166 support staff

28 affiliates

Key Publications

A sampling of the articles, books, guides, papers, and reports published by SEI staff in FY 2006. A complete list is online at www. sei.cmu.edu/annual-report.

Journal Articles

Amirijoo, M.; Hansson, J.; & Son, S. "Specification and Management of QoS in Real-Time Databases Supporting Imprecise Computations." *IEEE Transactions on Computers* 55, 3 (March 2006): 304-319.

Bloomfield, R.; Guerra, S.; Miller, A.; Masera, M.; & Weinstock, C. "International Working Group on Assurances Cases (for Security)." *IEEE Security and Privacy* 4, 3 (May/June 2006): 66-68.

Chaki, S.; Clarke, E.; Ouaknine, J.; Sharygina, N.; & Sinha, N. "Concurrent Software Verification with States, Events and Deadlocks." *Formal Aspects of Computing Journal (FACJ)* 17, 4 (December 2005): 461-483.

Clements, P.; Jones, L.; McGregor, J.; & Northrop, L. "Project Management in a Software Product Line Organization," *IEEE Software*, (September/October 2005): 54-62.

Greenhouse, A.; Halloran, T. J.; & Sherlis, W. "Observations on the Assured Evolution of Concurrent Java Programs." *Science of Computer Programming* 58, 3 (December 2005): 384-411.

Groce, A.; Chaki, S.; Kroening, D.; & Strichman, O. "Error Explanation with Distance Metrics." *International Journal on Software Tools for Technology Transfer (STTT)* 8, 3 (June 2006): 229-247.

Kazman, R.; Klein, M.; & Bass, L. "The Essential Components of Software Architecture Design and Analysis." *Journal of Systems and Software*, 79 (2006): 1207-1216.

Kazman, R.; Bass, L.; Klein, M.; Lattanze, T.; & Northrop, L. "A Basis for Evaluating Software Architecture Analysis Methods." *Software Quality Journal*, 13 (2005): 329-355.

Lewis, G.; Morris E.; & Smith, D. "Migration of Legacy Components to Service-Oriented Architectures." *The DoD SoftwareTech News 8*, 3 (October 2005).

Nord, R. & Tomayko, J. "Software Architecture-Centric Methods and Agile Development." *IEEE Software* 23, 2 (March/April 2006).

Scacchi, W.; Feller, J.; Fitzgerald, B.; Hissam, S.; & Lakhani, K.; eds. Special Issue on Free or Open Source Software Development (F/OSSD) Projects, J*ournal of Software Process: Improvement and Practice (SPIP)*, (May 2006).

Schmerl, B.; Aldrich, J.; Garlan, D.; Kazman, R.; & Yan, H. "Discovering Architectures from Running Systems." *IEEE Transactions on Software Engineering* 32, 7 (July 2006).

Books

Humphrey, W. *TSP: Coaching Development Teams*. Boston, MA: Addison-Wesley Professional, 2006.

Guides

Feiler, P.; Gluch, D.; & Hudak, J. *The Architecture Analysis & Design Language (AADL): An Introduction*. (CMU/SEI-2006-TN-011).

Conference Papers

Chaki, S. "SAT-Based Software Certification," 151-166. *Proceedings of the 12th International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS)*, March 25-April 2, 2006.

Chaki, S.; Clarke, E.; Kidd, N.; Reps, T.; & Touili, T. "Verifying Concurrent Message-Passing C Programs with Recursive Calls," 334-349. *Proceedings of the 12th International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS)*, March 25-April 2, 2006.

Chaki, S.; Clarke, E.; Grumberg, O.; Ouaknine, J.; Sharygina, N.; Touili, T.; & Veith, H. "State/Event Software Verification for Branching-Time Specifications," 53-69. *Proceedings of the 5th International Conference on Integrated Formal Methods (IFM)*, November 29-December 2, 2005.

Hofmeister, C.; Kruchten, P.; Nord, R.; Obbink H.; Ran, A.; & America, P. "Generalizing a Model of Software Architecture Design from Five Industrial Approaches." *Proceedings of the Working IEEE/IFIP Conference on Software Architecture* (WICSA 5), 2005.

Nolan, R.; et al. "First Responders Guide to Computer Forensics." *First International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE 2005)*, Taipei, Taiwan, November 2005.

Rogers, L. "The CERT Survivability and Information Assurance Curriculum: Education for First Defenders." *10th Colloquium for Information Systems Security Education*, Boston, MA, June 7, 2006.

Reports

Bass, L.; Bergey, J.; Clements, P.; Merson, P.; Ozkaya, I.; & Sangwan, R. *A Comparison of Requirements Specification Methods from a Software Architecture Perspective*. (CMU/SEI-2006-TR-013).

Bass, L.; Nord, R.; Wood, W.; & Zubrow, D. *Risk Themes Discovered Through Architecture Evaluations*. (CMU/SEI-2006-TR-012).

Bergey, J. & Cohen, S. *Product Line Acquisition in a DoD Organization—Guidance for Decision Makers*. (CMU/SEI-2006-TN-020).

Brownsword, L.; Fisher, D.; Morris, E.; Smith, J.; & Kirwan, P. *System-of-Systems Navigator: An Approach for Managing System-of-Systems Interoperability*. (CMU/SEI-2006-TN-019).

Caralli, R.; et al. *Sustaining Operational Resiliency: A Process Improvement Approach to Security Management*. (CMU/SEI-2006-TN-009).

Chaki, S. *SAT-Based Software Certification*. (CMU/SEI-2006-TN-004).

Chaki, S. & Hissam, S. *Certifying the Absence of Buffer Overflows*. (CMU/SEI-2006-TN-030).

CMMI Product Team. *CMMI for Development, Version 1.2*. (CMU/SEI-2006-TR-008).

Davis, N. *Secure Software Development Life Cycle Processes: A Technology Scouting Report*. (CMU/SEI-2005-TN-024).

Dodson, K.; Hofmann, H.; Ramani, G.; & Yedlin, D. *Adapting CMMI for Acquisition Organizations: A Preliminary Report*. (CMU/SEI-2006-SR-005).

Firesmith, D. QUASAR: *A Method for the QUality Assessment of Software-Intensive System ARchitectures*. (CMU/SEI-2006-HB-001).

Fisher, D. *An Emergent Perspective on Interoperation in Systems of Systems*. (CMU/SEI-2006-TR-003).

Gibson, D.; Goldenson, D.; & Kost, K. Performance Results of CMMI-Based Process Improvement. (CMU/SEI-2006-TR-004).

Hayes, W.; Miluk, G.; Ming, L.; Glover, M.; & Members of the SCAMPI B and C Project. *Handbook for Conducting Standard CMMI Appraisal Method for Process Improvement (SCAMPI) B and C Appraisals, Version 1.1*. (CMU/SEI-2005-HB-005).

Hissam, S.; Moreno, G.; & Wallnau, K. *Using Containers to Enforce Smart Constraints for Performance in Industrial Systems*. (CMU/SEI-2005-TN-040).

Humphrey, W. *Safety-Critical Systems and the TSP*. (CMU/SEI-2005-TN-011).

Kazman, R. & Bass, L. *Categorizing Business Goals for Software Architectures*. (CMU/SEI-2005-TR-021).

Keeler, K. *U.S. Army Acquisition—The Program Office Perspective*. (CMU/SEI-2005-SR-014).

Lapham, M. S*ustaining Software-Intensive Systems*. (CMU/SEI-2006-TN-007).

Lewis, G.; Morris, E.; O'Brien, L.; Smith, D.; & Wrage, L. *SMART: The Service-Oriented Migration and Reuse Technique*. (CMU/SEI-2005-TN-029).

Lewis, G. & Wrage, L. *Model Problems in Technologies for Interoperability: Web Services*. (CMU/SEI-2006-TN-021).

Marz, T. *Integrated Diagnostics: Operational Missions, Diagnostic Types, Characteristics, and Capability Gaps*. (CMU/SEI-2005-TN-035).

Muller, H.; O'Brien, L.; Klein, M.; & Wood, B. *Autonomic Computing*. (CMU/SEI-2006-TN-006).

Novak, W., ed. *Software Acquisition Planning Guidelines*. (CMU/SEI-2005-HB-006).

Siviy, J.; Penn, M. & Harper, E. *Relationships Between CMMI and Six Sigma*. (CMU/SEI-2005-TN-005).

Ward, M.; Elm, J.; & Kushner, S. *Techniques for Developing an Acquisition Strategy by Profiling Software Risks*. (CMU/SEI-2006-TR-002).

Woody, C., et al. *Applying OCTAVE: A Practitioner's Report*. (CMU/SEI-2006-TN-010).

Opportunities

Are you interested in being part of a world-class organization, accelerating adoption of software engineering best practices, or delivering those best practices? The SEI offers opportunities for organizations and individuals to participate in our transition services, research, and conferences. Below are ways that you can connect with the SEI.

SEI Guide to Products and Services

The SEI Guide to Products and Services is a complete catalog of all the SEI's tools and methods, services, courses, conferences, credentials, books, and opportunities to collaborate with the SEI on research. To receive a copy of the Guide, please contact:

Customer Relations
Software Engineering Institute
Carnegie Mellon University
4500 Fifth Avenue
Pittsburgh, PA 15213-2612
1-888-201-4479 or 412-268-5800
customer-relations@sei.cmu.edu

See the Guide to Products and Services online at **www.sei.cmu.edu/publications**.

Shane McGraw   **Deen Blash**

SEI Customer Relations representatives Shane McGraw and Deen Blash received and responded to about 25,000 inquiries in FY 2006 from both U.S. and overseas customers. Both Blash and McGraw, who combined have more than a decade of experience in customer relations, say that a thorough knowledge of the SEI's technical and outreach programs is the best way to respond quickly and accurately to all inquiries. Their average response time this year was about 20 minutes for inquiries received during business hours.

How the SEI Works with Government and Industry

SEI staff members help the Department of Defense and other government agencies solve software engineering and acquisition problems. Engagements with the SEI are of particular benefit to government program managers, program executive officers, and senior acquisition executives. The SEI also works with commercial organizations that want to mature new technology for the benefit of the entire software industry and with those that want to develop a strategic advantage by rapidly applying improved software engineering technology.

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

SEI Employment

The SEI seeks candidates for its technical engineering and business divisions. Contact our Human Resources department to learn the benefits of working at the SEI: **www.sei.cmu.edu/about/employment/employment.html**.

To download a PDF version of this annual report, go to
www.sei.cmu.edu/annual-report

Software Engineering Institute
Carnegie Mellon University
4500 Fifth Avenue
Pittsburgh, PA 15213-2612
Phone: 412-268-5800
Toll-free: 1-888-201-4479
Fax: 412-268-5758
www.sei.cmu.edu
customer-relations@sei.cmu.edu
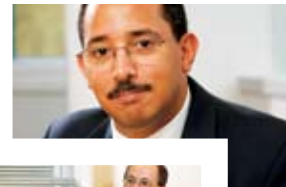
SEI Europe
An der Welle 4
Reception Level 1
60322 Frankfurt
Germany

SEI Huntsville
AMSAM-BA
Building 6263
Redstone Arsenal, AL 35898

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

SEI Los Angeles
6th Floor
400 Continental Boulevard
El Segundo, CA 90245

SEI Colorado Springs
Suite 111
1155 Kelly Johnson Boulevard
Colorado Springs, CO 80920