THE MONITOR

CERT Team Examines Health-Care Security Risks

In April 2009, newspapers were dominated with headlines about intruders breaking into a Virginia state website that pharmacists used to track prescription drug use. The intruders allegedly deleted records of more than 8 million patients and replaced the site's home page with a ransom note demanding $10 million.

Six months earlier, Express Scripts, one of the largest pharmacy benefit management companies in North America, announced that it had received a letter from an unknown person or persons trying to extort money from the company by threatening to expose millions of the company's patient records.

On a separate front, the federal government has made electronic medical records a national priority. In fact, the Health Information Technology for Economic and Clinical Health (HITECH) Act, a component of the American Recovery and Reinvestment Act (ARRA) of 2009, has mandated the widespread adoption and use of electronic health record (EHR) technologies. Health-care organizations now face the challenge of protecting patient information while minimizing the risks posed by this new requirement.

The issue has become a primary source of concern among health-care providers. According to a survey released in August by Imprivata Inc., 76 percent of organizations claim "breach of confidential information or unauthorized access to clinical applications" as their greatest security concern, and yet 38 percent report that they cannot track inappropriate access in accordance with the HITECH Act.

Far too often, the threats come from within an organization, according to Randy Trzeciak, a senior member of the technical staff at CERT and the insider threat team lead. Since its inception, the CERT insider threat team has studied internal malicious activity against organizations. The team has created a database of more than 400 insider threat cases that team members use to analyze potential indicators of malicious activity. The insider threat team has identified three types of insider threat crime:

- IT sabotage: An insider(s) sabotages systems or data to cause some harm to an organization.
- theft of intellectual property: An insider(s) steals confidential or sensitive information.
- fraud: An individual(s) modifies, adds, or deletes data from a database. This type of crime also includes individuals stealing large sets of data from an organization and selling that data to external parties, resulting in fraud (e.g., identity theft, credit card fraud) against the victims.

continued on page 3

SEI Members from left: Kristal Ray of Oracle, Carmela Rice of the U.S. Army, Michael P. Robillard of McKesson, and Michele Lamptey Urich of Northrop Grumman. Thanks to Anna Mosesso for contributing photography.

Go paperless! If you would like to receive an email containing a PDF version of *The Monitor* instead of a printed version, email membership@sei.cmu.edu.

SEI Membership
Carnegie Mellon University
4500 Fifth Avenue
Pittsburgh, PA 15213-2612
412-268-5800
Toll-free: 888-201-4479
Email: **membership@sei.cmu.edu**
www.sei.cmu.edu/membership

The Latest from the SEI: Chief Technology Officer Doug Schmidt

In his new role as deputy director, research, and chief technology officer of the Carnegie Mellon Software Engineering Institute, Dr. Douglas C. Schmidt will lead the SEI in identifying and responding to the needs of sponsors, customers, and partners. An important aspect of his role will focus on advancing the scope and impact of SEI research.

"One of the biggest challenges—and opportunities for future growth—that we face at the SEI is achieving the right balance and synergy between research and transition," explained Schmidt, who comes to the SEI from Vanderbilt University, where he was a tenured professor and served as associate chair of the Department of Electrical Engineering and Computer Science. "By expanding the depth and breadth of our research programs, the SEI will be better positioned to shape future innovations in complex software-reliant systems," Schmidt continued. "Likewise, we will be more effective in providing the technical leadership and mentoring needed to advance the practice of software engineering in acquisition programs."

Schmidt has a wealth of experience managing software research and development programs. He was a deputy office director and a program manager in the Information Technology Office and Information Exploitation Office at the Defense Advanced Research Projects Agency (DARPA), where he led the national research and development effort on software technologies for large-scale distributed real-time and embedded (DRE) systems. He also co-chaired the Software Design and Productivity (SDP) Coordinating Group of the U.S. government's multi-agency Information Technology Research and Development (IT R&D) Program, which formulated the national multi-agency software research agenda. In addition, he served as chief technology officer at both Zircon Computing and Prism Technologies, where he was responsible for the companies' technical vision, strategic directions, and growth.

To help the SEI achieve the necessary balance and synergy between research and transition, Schmidt plans to leverage new technologies, including a web-based repository—sponsored by the DoD's Director, Defense Research and Engineering (DDR&E) office—that serves as a virtual collaboration point for DoD software developers, users, and software engineering researchers on key challenges faced in software producibility, verification, and validation by acquisition programs.

"You can think of this repository as an 'eHarmony' -like collaboration portal that matches researchers who have innovative solutions with acquisition programs that must resolve vexing software problems," Schmidt said, adding that he plans to continue populating the repository based on needs that the SEI encounters when working with organizations in acquisition support engagements.

On a second front, Schmidt said that the web-based repository could serve as another means to showcase how cutting-edge SEI research initiatives are solving hard acquisition problems. "This approach has the opportunity to dramatically reshape the way that software research is conducted for the DoD, as well as more broadly influence the software engineering R&D community." Schmidt said that the resulting collaborations will not only help integrate SEI programs internally, but also help the SEI partner more effectively with other research facilities, including universities, federally-funded research and development centers, and DoD system integrators.

During the past decade, Schmidt said, there has been a movement throughout the DoD and industry toward so-called "effects-based management" of research portfolios, which places emphasis on "smart" (streamlined, measurable, actionable, real, and timely) research that combines advances in fundamental theories and methods with clearly defined success criteria that matter to transition stakeholders. Schmidt is making this style of portfolio management a priority to increase the visibility of SEI research in high-impact journals, conferences, and trade publications, as well as to ensure that the output of SEI research (such as tools and related software artifacts, datasets/benchmarks, demonstrations, and standards) make a significant contribution to the warfighter.

"The SEI has done groundbreaking work for many years. We need more opportunities for our sponsors, partners, and users to see the work that we do," Schmidt explained. "One of the things that has held software engineering back for a long time, as compared to other disciplines, is that we have a very hard time quantifying the impact of our research and tracking our progress in tangible terms."

For several decades, computer science and software engineering research was given a "free ride," so to speak, because information technologies (IT) were evolving so rapidly and the novelty of computing promoted an unfettered research agenda and funding environment, explained Schmidt. As the computing industry matures and becomes more of a commodity, however, this free ride is over. "Now we are no longer the new kids on the block," he said, adding that researchers in other science and engineering disciplines have been more effective in articulating the need for—and progress resulting from—their methods and contributions. One result of the perceived commoditization of IT is that there has been a decline in funding for research in computer science and software engineering over the past decade. Too often, important sponsors in government believe that commercial industry alone will solve all the software challenges faced by the DoD. "The DoD has some incredibly important software needs that will not be met easily by the commercial world without help from the SEI and others in the research community," said Schmidt.

Other priorities for Schmidt are increasing the SEI's emphasis in the fields of agile methods that complement and leverage existing work on CMMI and TSP, ultra-large-scale system technologies and socio-technical ecosystems that extend the SEI's work in software architecture and productlines, and trustworthy mobile computing for the tactical edge. "At the other end of the spectrum, there is a huge movement toward cloud computing," Schmidt said. "More and more computing will be done in public and/or private clouds, and the DoD needs the SEI's help to ensure that these clouds are secure, scalable, dependable, and affordable."

To read more about Schmidt:
www.sei.cmu.edu/newsitems/SEI-Announces-New-Chief-Technology-Officer.cfm

CERT Team Examines Health-Care Security Risks, continued

According to Trzeciak, health-care organizations are at risk because of the nature of information that they collect. That risk often originates from within, and is primarily the result of fraud.

"If you look at information that health-care providers collect on patients, in many cases it is information that is personally identifiable. There could be a market for that particular data, which individuals could use to commit some type of identity theft," explained Trzeciak, adding that all organizations, not just those in health care, collect similar information about their employees.

With each passing year, medical facilities and hospitals rely more heavily on IT systems. This reliance makes them vulnerable to IT sabotage, which is often perpetrated at the hands of an employee. "Employees who conduct IT sabotage are disgruntled. There is a perceived injustice on the part of the individual. Often, there has been a negative workplace event that caused the person to become disgruntled and want to exact revenge against the organization," Trzeciak said.

Greg Porter, a visiting scientist at CERT and the founder of Allegheny Digital, a security and privacy services company based in western Pennsylvania, said there are many avenues where a breach of information can occur, including social media. And, he added, while health-care entities are more rapidly adopting new technologies, they often lag behind when it comes to securing those technologies.

"If ad hoc security management rules the day, as it does in plenty of health-care organizations, it's just a matter of time until a breach occurs," Porter said. The resulting breach can cause serious consequences beyond legal fees. What if the IT system that is compromised is connected to a patient monitoring system? "People often focus on the data, health information itself, as they should, but consideration must also be given to critical internal systems, such as an IV infusion pump in the intensive care unit (ICU), that could be supporting a human life. What are the consequences if the integrity of those assets is compromised?"

To further complicate matters, the security and privacy regulations called for in the HITECH Act now apply not only to health-care organizations, but the businesses that work with them.

"Business associates such as claims processors and medical transcription companies are all becoming quite concerned—and rightfully so. Information security isn't their specialty; it's not part of their core business. But without the right oversight, medical information can become exposed," explained Porter.

Porter said that he wanted to collaborate with CERT because of programs such as secure coding, resilience management, and insider threat where researchers are working to address these issues.

The CERT insider threat team has developed a number of resources to help organizations. These resources, available from the insider threat area of the CERT website, include "The Common Sense Guide to Prevention and Detection of Insider Threats," which outlines 16 steps that organizations can take to respond to insider malicious activity.

For more information about this work, visit www.cert.org/insider_threat/.

Randy Trzeciak and Greg Porter presented a webinar on September 23, 2010 as part of the SEI Webinar Series. The two discussed the effects of the recent regulations on the health-care industry and some of the essential elements that health-care technology executives should consider to secure patient information and systems from external threats. Porter will also discuss the synergies between the HITECH Act's breach notification requirements and incident response programs.

To view an on-demand production of the webinar, visit www.sei.cmu.edu/library/webinars.cfm

Noteworthy Technical Reports

THE FOLLOWING SEI TECHNICAL REPORTS HAVE BEEN RECENTLY PUBLISHED. PLEASE VISIT THE ACCOMPANYING URLS TO DOWNLOAD A FREE COPY.

Measurement and Analysis Infrastructure Diagnostic, Version 1.0: Method Definition Document

By Mark Kasunic
www.sei.cmu.edu/library/abstracts/reports/10tr035.cfm

COVERT: A Framework for Finding Buffer Overflows in C Programs via Software Verification

By Sagar Chaki & Arie Gurfinkel
www.sei.cmu.edu/library/abstracts/reports/10tr029.cfm

A Framework for Modeling the Software Assurance Ecosystem: Insights from the Software Assurance Landscape Project

By Lisa Brownsword, Carol Woody, Christopher J. Alberts, & Andrew P. Moore
www.sei.cmu.edu/library/abstracts/reports/10tr028.cfm

Risk Management Framework

By Christopher J. Alberts & Audrey J. Dorofee
www.sei.cmu.edu/library/abstracts/reports/10tr017.cfm

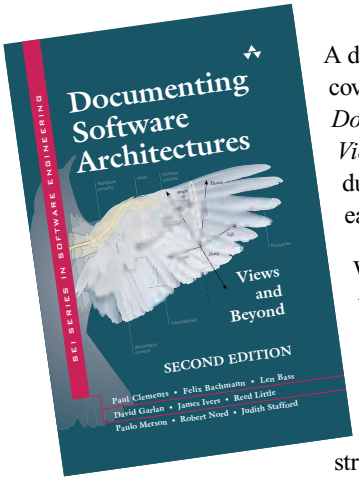
Lessons Learned from a Large, Multi-Segment, Software-Intensive System

By John T. Foreman & Mary Ann Lapham
www.sei.cmu.edu/library/abstracts/reports/09tn013.cfm

Incremental Development in Large-Scale Systems: Finding the Programmatic IEDs

By Charles (Bud) Hammons
www.sei.cmu.edu/library/abstracts/reports/09tn015.cfm

The Latest Book from the SEI: Documenting Software Architectures



A diagram of a bird's wing spans the cover of the latest book from the SEI, *Documenting Software Architectures: Views and Beyond, Second Edition*, due out from Addison-Wesley in early October.

Why such an organic structure on the cover of a decidedly technical book? Paul Clements, co-author of the book and a senior member of the technical staff at the SEI, explained: "In a physiological structure such as a bird's wing, you have bone, nerve, and circulatory structures all coming together to perform in unique ways. The result is much more than the sum of its parts. The same is true of systems and software architectures."

The book is written to give users the tools that they need to clearly communicate about software and systems architectures. If architectures are not effectively communicated, the effort that went into documenting them will have been for naught, Clements explained.

"The purpose of this new edition is to answer the question 'How do you successfully document an architecture?'" Clements said. "What do you need to say about your architecture so that other people can use it effectively?"

In keeping with that purpose, this practitioner-focused edition includes

- an emphasis on working software over comprehensive documentation—a tenet of the Agile Manifesto
- three appendices on languages for documenting architectures: Unified Modeling Language (UML) 2.0, Systems Modeling Language (SysML), and Architecture Analysis and Design Language (AADL). Each of those appendices is a mini-reference guide to the language from the perspective of using it to capture an architecture.
- updated templates for architecture documentation that provide new layout options
- a new chapter on reviewing an architecture document to ensure that it is serving the goals of stakeholders
- guidance on the architecture-level documentation of a software system's data model
- examination of service-oriented architectures, multi-tier architectures, and architectures for aspect-oriented systems

Clements said that he and his co-authors worked hard to be sure that the book communicates effectively too. On each page, they present the information in a way that is engaging and visually appealing.

"We have more than 200 figures and several dozen tables. We made a conscious effort to make sure that if you open the book to any page, you will not just see two pages of text," Clements said.

Documenting Software Architectures: Views and Beyond, Second Edition by Paul Clements, Felix Bachmann, Len Bass, David Garlan, James Ivers, Reed Little, Paulo Merson, Robert Nord, and Judith Stafford is part of the SEI Series in Software Engineering published by Addison-Wesley. This book is available beginning October 8. For more information: www.informit.com/store/product.aspx?isbn=0321552687

The SEI's Ask the Expert

SEI Membership introduces a new feature in which Deen Blash, SEI Membership team lead and expert at what's out there on the SEI website, answers a reader's question.

To submit your question for the November edition of The Monitor, please email membership@sei.cmu.edu.

Question:
Where can I find the latest information on CMMI Version 1.3?

Answer:
To provide you with the latest news about CMMI Version 1.3, we have created a CMMI V1.3 information center on the SEI website. All of the latest information will be posted here as it becomes available: www.sei.cmu.edu/cmmi/tools/cmmiv1-3.

A download of the current CMMI V1.3 Quick References is available at https://bscw.sei.cmu.edu/pub/bscw.cgi/d868800. These references show the process areas, purpose statements, goals, specific practices, and generic goals and practices as they will appear in V1.3. We have provided a separate reference for each of the three CMMI models.

The first offering of CMMI V1.3 Model Upgrade Training will be held during the CMMI Workshop, October 4-6 in Las Vegas. An online version of the training will be available in January. Workshop registration is closed, but we are considering at least one more face-to-face offering between October and January. We are interested in your needs for a face-to-face offering. Please tell us the location and date that works best for you at http://sei.qualtrics.com/SE?SID=SV_3ZQce2TOOmT75Ig .

Write to cmmi-comments@sei.cmu.edu to ask questions or give input on CMMI V1.3; your questions help us to know what information to provide next.

Member Profile

Bill Flury

Member Since January 2006
email: bflury@verizon.net

SEI Member Bill Flury worked on application development teams at the National Security Agency (NSA), Office of Naval Intelligence, GE, and RCA when they were building and fielding the very first military intelligence applications.

Fresh out of Princeton with a degree in Oriental Languages, he worked as a civilian cryptanalyst at the National Security Agency. There, with the help of some very early ADP equipment (including an IBM 101) he was able to achieve some significant success.

After he left the NSA, Flury enlisted in a Navy officer candidate school program and was assigned to the pentagon where he served as a current intelligence briefer on the Middle East for the Chief of Naval Operations.

In addition to his briefing duties, he worked with the Navy application development teams to create and populate several database applications. These included apps for keeping track of hundreds of foreign government officials; managing security clearance records; monitoring the movements of foreign merchant ships in the Atlantic; and an app to support Navy and Coast Guard responses to SOS calls using large-screen displays.

In 1964 Flury was part of the group that started MITRE Washington. He continued to develop database applications in support of the Joint Chiefs of Staff. His work on designing and developing a reporting system and planning model for managing the flow of munitions and herbicides to Vietnam was commended by the Secretary of Defense for saving the Department of Defense more than $3 million a day.

During the last two years of the Carter administration and the first two years of the Reagan administration, Flury said that he and his team worked to develop and install the first computer applications and train the White House staff on their use.

Working out of an office in the Eisenhower Executive Office building, Flury said he spent most of his time in the west wing of the White House developing management applications to support senior staff.

"Sitting in meetings in the west wing with people who are special assistants to the President is a fun job," Flury recalled.

After MITRE, Flury worked for eight years at SRA International, where he served as deputy director of the Defense Systems group. One major effort of this group was to collect, document, and manage the requirements for the Army WWMCCS system.

At that time the Joint Staff increased the emphasis on combining and integrating separately developed, but related, applications into complete systems. There were more than 225 separately developed and funded military logistics systems, and they could not readily "talk" to each other. Flury and two logistics specialists took on the task of figuring out to integrate these systems. They became the architects of what was first called the Joint Operations Execution System (JOPES) which, by the time of its achievement of full operational capability 13 years later, had morphed into the Global Command and Control System (GCCS).

"Sitting in meetings in the west wing with people who are special assistants to the President is a fun job."

Since retiring in 1996, Flury has been an independent consultant. As an adjunct professor at American University, he has taught software project management and engineering, human factors in information systems, systems engineering, and the graduate seminar in information systems.

Flury qualified early-on to participate in CMM appraisals and has worked with the Center for Systems Management and iPower LLC to build their improvement practices. He just participated in his first CMMI for Services SCAMPI.

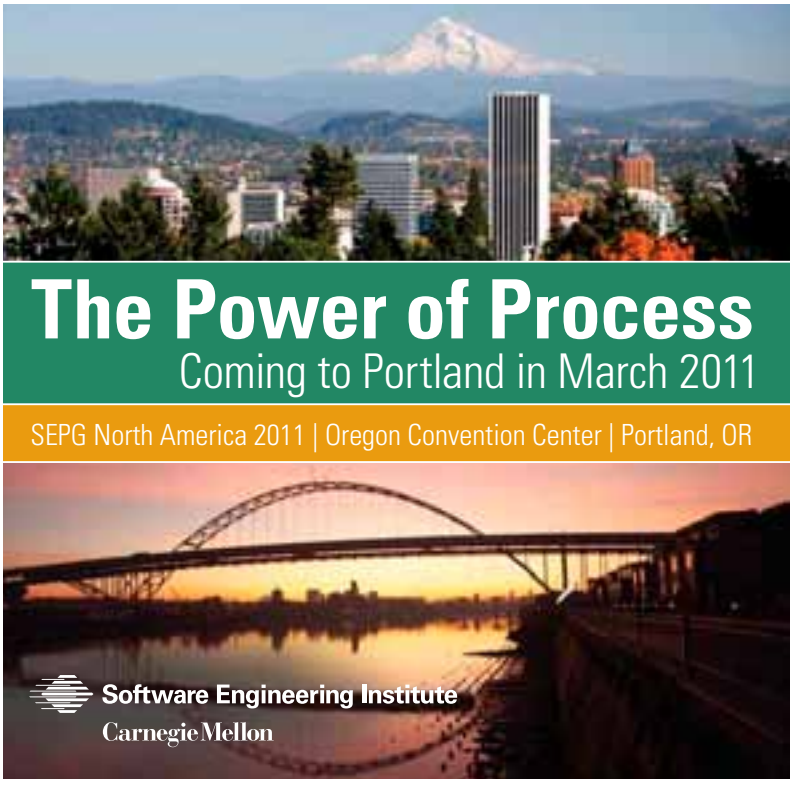
In his latest incarnation, he is working with Chris Fristad, also an SEI Member, to develop a new website that makes available checklists that the two have found useful to achieve success in projects. "We felt with our accumulated experience that we could produce checklists that would be useful to a lot of people," Flury explained.

Flury became an SEI Member in January 2006. "The Member program has been a wonderful resource for the kinds of things that interest me; and as you can tell, I have a lot of interests," Flury said.

SEI Membership | Carnegie Mellon

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

SEPG NORTH AMERICA 2011 CALL FOR PARTICIPATION



Open Now Through October 29, 2010

Do you have real-world examples, lessons learned, innovative ideas, or an exciting perspective on a cutting edge topic that you'd like to share with the software process improvement community? Do you want to participate in the SEPG North America 2011 conference—which will be held March 21 -24, 2011 in Portland, Oregon—and help promote the power of process by speaking or reviewing abstracts?

This year's Call for Participation focuses on the critical challenges and issues in process improvement and how we can harness the power of process to implement smart solutions.

The Call for Participation is now open until midnight on **October 29, 2010**. Individuals interested in submitting an abstract for consideration should first review the SEPG North America 2011 call for papers page at www.sei.cmu.edu/sepg/na/2011/call.cfm