Software Engineering Institute
Carnegie Mellon

Attacking Network and Software Complexities:
Tools for the Cyber Warrior

Software Engineering Institute

On behalf of the Software Engineering Institute, welcome to LandWarNet.

The Software Engineering Institute—the SEI—is a Department of Defense federally funded research and development center (DoD FFRDC). Our mission: advance software engineering and related disciplines to ensure predictable and improved quality, schedule, and cost in the development and operation of software-reliant DoD systems.

We do this through research and technology transition involving the DoD, federal agencies, industry, and academia. Specifically, we emphasize high quality research that benefits the DoD by identifying and solving key technical challenges facing current and future DoD software-reliant systems.

A distinguishing feature of the SEI's research is its twin focus on innovation and utility:

The SEI's research is **innovative** because it

- blazes new trails, rather than just filling gaps in knowledge
- builds new concepts and paradigms, as well as new kinds of engineering solutions
- finds promising solutions to problems that are rising in importance

The SEI's research is **useful** because

- research results provide significant utility to the community
- research results are adopted by practitioners who then achieve measurable improvements in their software engineering practices

Overall, the SEI's work follows two thrusts: one thrust focuses on advancing the state of knowledge by *exploring and creating* new methods, techniques, and tools, while the second thrust focuses on improving the utility of these research results by *applying and amplifying* them.

The SEI's high quality research staff is applying its efforts to four major areas of interest:

- innovating software for competitive advantage
- securing the cyber infrastructure
- advancing quantitative methods for engineering software
- accelerating assured software delivery and sustainment for the mission

The work encompasses expanding knowledge and understanding of software-reliant systems; multi-core processors; software security; quantitative models, measurement, and management methods; and more. It also includes creating potential new areas of research through an exploratory process that encourages researchers to tackle hard problems and emerging research questions.

I hope you'll take this opportunity, at LandWarNet, to learn more about the SEI. Please feel free to come by our booth and talk to our people—they'd be happy to help you or put you in contact with a person or team at the SEI who can.

Best regards,

Dr. Douglas C. Schmidt
Deputy Director, Research
Chief Technology Officer
The Software Engineering Institute

P.S.: For the latest thinking on today's challenges in software engineering, be sure to check out our blog at http://blog.sei.cmu.edu, and our website at http://www.sei.cmu.edu.

Carnegie Mellon

CERT Team Uses XNET to Deliver Authentic Forensics Challenge at CDX 2011

An international aid organization website suffers a cyber attack. The host nation's information assurance team quickly determines the attackers stole critical information from a database on the server. They also planted malware to enable them easy access in future attacks. Later, the team learns a taskforce in the field has captured a computer believed to have been part of the attack. From the suite of analysis tools available in the CERT® Forensic Appliance, the team employs LiveView to create a bootable image of the captured computer and begins forensic analysis. But the team soon encounters a roadblock: All the computer's files are rendered in a foreign language. How can the team deconstruct the attack?

This scenario—the CERT Forensics Challenge—was designed by CERT for the 2011 National Security Agency (NSA) Cyber Defense Exercise (CDX). CERT has played a key role in this competition since its inception in 2001. The CDX pits teams of information assurance students from the nation's service academies against cyber security experts from the NSA. Each student team designs and implements a test network on its campus and, during the four-day exercise, works to defend it against cyber attacks from the NSA. Judges score the teams on their ability to successfully defend their networks and information.

To make the CERT Forensics Challenge both difficult and authentic, CERT tapped its expertise in the field of computer forensics and its long experience supporting DoD activities. It also employed its sophisticated Exercise Network (XNET) environment. CERT created XNET to provide real-world readiness testing through synchronous, team-based, scenario-driven cyber exercises. In other words, it's a platform ideally suited for the CDX.

Brian Wisniewski knows the CDX well. As Mission Support Team chief for the Army Reserve Information Operations Command, he led detachments supporting the NSA in several previous CDX events. Wisniewski, who in civilian life is also a member of the CERT Cyber Exercise team, found himself perfectly placed to introduce the CERT Forensics Challenge to CDX 2011. "This was a great opportunity to work with NSA to build a scenario that fits their CDX directive and scoring model," noted Wisniewski. "Overall, the Forensics Challenge was very well received. More than one institution mentioned that it was positioned at just the right level."

Wisniewski credits the success of the Forensics Challenge to the dedication and creativity of his fellow team members. For instance, Brent Kennedy developed a multiple-enclave technology map for the challenge. This tool allowed CDX observers to drill down through a graphical representation during the exercise, providing them a view into the activities of the attacking and defending teams. According to Wisniewski, the CDX observers found this tool useful because it showed them in real time how team members were applying classroom knowledge to problem solving.

Other CERT contributors included Matt Kaar, who created the foreign-language sleight of hand intended to distract the teams from their standard analytical and problem-solving processes. Jeff Mattson and Leena Arora helped Wisniewski create the challenge scenario and provided on-site support. "The challenge gave us an excellent opportunity to highlight the capabilities of the entire CERT Workforce Development team," said Wisniewski. It also provided the service academy teams with experience with CERT-developed tools, such as those available in the CERT Forensics Tools Repository and LiveView.

Major T.J. O'Connor, director of the U.S. Military Academy's (West Point's) Digital Forensic and Computer Exploitation Courses, sees great value in the CERT Forensics Challenge. "The CDX challenge created by Brian's team was outstanding and helped reinforce what the cadets had learned in the classroom," said O'Connor. "What impressed me the most was the realism of the challenge. Having previously served overseas, I can honestly state Brian's team replicated the environment rather well." O'Connor specifically cited the way in which the CERT XNET environment incorporated real-world places, databases, unit identifiers, and other details the cadets will likely encounter in their future roles.

"To master the challenge," noted O'Conner, "the cadets had to have a full understanding of network forensics, file system forensics, analysis of metadata, and information-hiding techniques. The breadth of the skills necessary to master the challenge was impressive. Having participated in three previous Cyber Defense Exercises, I can say without a doubt that this was the most realistic challenge the cadets have experienced to date."

To the winner go the bragging rights, and this year O'Connor's team took the title. The CDX, however, is more than a competition—it's an exercise designed to prepare future leaders in cyber defense in a realistic, live-fire environment. The CERT Cyber Exercise Team developed the Forensics Challenge with this in mind and learned much in the process. It will use the lessons it learned from CDX 2011 to enhance XNET with new, authentic training scenarios.

Related Web Sites

To learn more about XNET, visit http://xnet.cert.org/xnet1/.

To learn more about computer forensics at CERT, visit http://www.cert.org/forensics/.

For General Information

For information about the SEI and its products and services, contact
Customer Relations
Phone: 412-268-5800
FAX: 412-268-6257
customer-relations@sei.cmu.edu
www.sei.cmu.edu

8/2/2011

Information Sheet
Network Situational Awareness

Cyber Threat and Vulnerability Analysis Directorate
Software Engineering Institute
Carnegie Mellon University
netsa-contact@cert.org
http://www.cert.org/netsa/

Mission

Improve Internet security by detecting threats early, and sharing data in near real-time. Play an active role in providing the knowledge and capacity to secure and monitor valuable networks through:

Applied Research and Development *- Design and implement gap capabilities for current sensor and analysis tools ("works in the real world")*

Operational Analysis - *Conduct strategic studies and tactical analyses for operational organizations ("learn by doing")*

Capacity Building *- Grow a community of analysts through open source software, standards, publication, and training ("show others")*

Capabilities

- **Access to Diverse Data**. We have access to a diverse set of data based on customer monitoring, other relationships and open source data sources: the CERT malware artifact catalog, and arrangements with other researchers such as the Internet Systems Consortium (ISC) and the Security Information Exchange (SIE) data set.
- **Operational Relationships**. We work directly with operational security groups in various parts of DoD, civilian and commercial, and understand operational analysis. We focus on community building, within and outside of government. We directly support the outreach and training program for DISA/NSA Community Data Center (CDC), Advanced Analysis and Training (A2T), providing technical direction, and work with analysts across DoD day-to-day with analysis help.
- **Community Building.** We run an annual network traffic analysis conference called "FloCon" that brings together the academic, research and operational communities. FloCon 2012 (http://www.cert.org/flocon/) will be held January 9-12, 2012, in Austin, TX.
- We also play a significant role in organizing and operating the regular CDC Centaur Technical Exchange (aka the "Jam Session").

- **DoD and Government Knowledge**. Our experience with DoD large-scale network analysis goes back over 8 years. Our technology remains the basis for the Centaur program. Over the years, we have built significant experience with DoD systems, networks and programs. We play a similar role in the providing expertise to DHS/US-CERT and the Einstein/NCPS program.
- **Software Development**. Based on operational linkages, our team develops new tools for large-scale sensing and analysis, supported by multiple government sponsors. Most of our tools are actively used in operations, running on very large networks. Our focus is addressing gaps left by commercial offerings. Efforts include high-performance standards-based network flow measurement and metadata extraction sensing software as well as tools for large-scale traffic analysis based on this collection.
- **Analysis Research**. We have extensive research depth as well as operational knowledge and experience. Practically the team consists of a mix of operational security professionals, developers, analysts and researchers. The relationship to Carnegie Mellon University and other programs in Software Engineering Institute means access to researchers in many cyber disciplines.
- **Scale/Practicality**. Our R&D is ultimately proven on real, very large-scale networks. We've got a lot of experience making analysis practical. There are no "magic alerting machines", just more useful indicators. We understand that. What we do is work with the community to make solutions that work on real networks, not just in the lab.
- **Expertise**. We have expertise in very large scale traffic analysis based on selective content inspection and header-based summaries (like netflow), significant experience analyzing DNS as well as expertise in general security analysis, engineering and architecture.
- **FFRDC Flexibility**. The Software Engineering Institute is a Federally Funded Research and Development Center. This enables CERT to play the role of an unbiased advisor, serving in a quasi-government role as needed to support program decisions.

References

The CERT/NetSA tools release site. http://tools.netsa.cert.org.

The FloCon Conference Web Site. http://www.cert.org/flocon/.

Centaurpedia. https://www.gsac[.smil].mil/centaurpedia. *Includes copies of various DoD reports released by the team and information about the Centaur technical exchange.*

Information Sheet
Software Testing
CERT® Basic Fuzzing Framework

Cyber Threat and Vulnerability Analysis Directorate
Software Engineering Institute
Carnegie Mellon University
cert@cert.org
http://www.cert.org/vuls/discovery/

June 2010

The CERT Basic Fuzzing Framework (BFF) is a software testing tool that can be used to find bugs in any software application that can run on the Linux platform. This framework was developed as part of the Vulnerability Discovery Project[1] in the CERT Coordination Center (CERT/CC) at Carnegie Mellon University's Software Engineering Institute (SEI). At the 2010 FIRST Conference, keynote speaker Mr. Phillip Reitinger, Deputy Undersecretary for the National Protection and Programs Directorate at the Department of Homeland Security, said the security community needs to focus on making software and hardware more secure as part of having "more healthy components in the cyber ecosystem." He said we need to design and create more secure components, realizing that although we will not obtain perfection, we can do much better. The CERT/CC is contributing that that effort by investigating ways to make software more reliable. While other parts of the SEI focus on reducing software defects by improving the software engineering process across the development lifecycle, one area of interest in the CERT/CC is to help software vendors and software developers identify and resolve vulnerabilities during the quality assurance phase before products are shipped.

The BFF runs within a VMware virtual machine and performs mutational fuzzing on a specified software application. Mutational fuzzing is the act of taking well-formed input data and corrupting it in various ways, looking for cases that cause crashes. The BFF automatically collects unique test cases that cause software to crash, as well as debugging information associated with the crashes. At the CERT/CC, we have already used the BFF infrastructure to find a number of critical vulnerabilities in products such as Adobe Reader, Flash, Foxit Reader, Apple QuickTime, Preview, xpdf, poppler, ffmpeg, jasper, Wireshark, VMware, and Indeo.

Applications crash because they have defects. Some defects are potentially vulnerabilities that individuals with malicious intent may be able to exploit. By using tools like the BFF, software developers can improve the quality of software, preferably before it ships to customers. Identifying the issues in advance reduces the time and expense that organizations need to invest to recover from these crashes. Developers of Linux software can easily access this framework by downloading it from the CERT website.[2] We have notified more than 800 vendors of the release and have encouraged them to use the framework. The United States government may also be able to benefit from using the BFF:

---

[1] http://www.cert.org/vuls/discovery/
[2] http://www.cert.org/download/bff/

- Organizations developing applications that run on Linux systems can test their software for defects or vulnerabilities.
- Organizations using third-party software that is available on Linux can test that software for defects and possible vulnerabilities as part of a security review of implications of using that software.

We welcome suggestions or feedback on the usefulness of the BFF. Please direct any feedback to cert@cert.org.

The BFF is just one of the CERT/CC's efforts in the area of vulnerability discovery. Other projects include the development of Dranzer, which is an ActiveX fuzzing tool, and an annual vulnerability discovery workshop.

CERT | Software Engineering Institute
Carnegie Mellon

CERT® Insider Threat Center Capabilities

It is critical that organizations detect indications and warnings of malicious insiders so that the crime never escalates to the next level. The CERT Insider Threat Center has spent the past decade researching insider fraud, theft of information, IT sabotage, and espionage, and transitioning that research into operational solutions for government and industry. The following tables outline our capabilities in terms of those that can be put to immediate use, those that can be accelerated to scale for widespread adoption, and longer-term research efforts.

Currently Available

Your Pain Points	CERT Insider Threat Center Solutions	Benefits to Your Organization
How can I become more aware of any organizational issues affecting my risk of insider threat?	• Insider threat workshops • Insider threat modules in our Virtual Training Environment (VTE)	• Greater understanding of the nature and prevalence of insider threat concerns and candidate countermeasures in an organizational context
How can I get better indications and warnings of malicious behavior and detect warning signs?	• Insider threat assessment	• More comprehensive protection, knowing that you are watching for the attack patterns of previous malicious insiders
How do I make the best use of my existing tools?	• Customized, tactical countermeasure guidance based on new operational controls from the CERT Insider Threat Lab	• Better situational awareness and improved security posture since tools are configured and properly tailored to the unique systems and concerns found in the mission operating environment • Cost savings - analysts' time is used more efficiently
Where can I get education and training for my staff to effectively deal with and diagnose insider attacks?	• Insider threat workshops • Insider threat executive workshop	• More effective incident response, reducing the likelihood that an insider attack will be missed, misdiagnosed, or dealt with inappropriately
Are my policies and procedures inhibiting detection and prevention of insider threats?	• Insider threat assessment • Insider threat executive workshop • Strategic action plan and supported execution	• Stronger ability to detect and respond to insider attacks, which will protect your organization and avoid compromises of assets, information, and reputation

www.cert.org/insider_threat

Acceleration to Scale

Your Pain Points	CERT Insider Threat Center Solutions	Benefits to Your Organization
How can more organizations become aware of organizational issues affecting their risk of insider threat?	• Training and certification of contractors to perform insider threat assessments • Espionage workshop (We have content that we could integrate into our regular workshop fairly quickly.) • Insider threat self-assessment tool • Espionage assessments (We could expand our insider threat assessment for a focused examination of insider threats in classified environments.)	• Identify issues in other organizations that could inhibit detection of insider threats
Where can I get training for my cyber analysts to effectively deal with and diagnose insider attacks?	• Cyber defense exercises conducted on the CERT exercise network (XNET)	• Technical security workforce more skilled in detecting indications and warnings of insider threat
How do I make the best use of my existing tools?	• Collaboration with vendor community results in enhanced automated tools • Operational test range • Insider threat implementation guides • Reference architecture(s)	• Reduced investigative burden from automated tools • Compliance can be measured against insider threat implementation guides • Consistent, shared tool evaluations
What policies, procedures, and technologies do I need for insider threat incident handling (prevent, detect, respond)?	• Insider threat incident handling guide • Insider threat standards	• Increased preparedness level for organizations to recognize, communicate, and respond to potential insider incidents

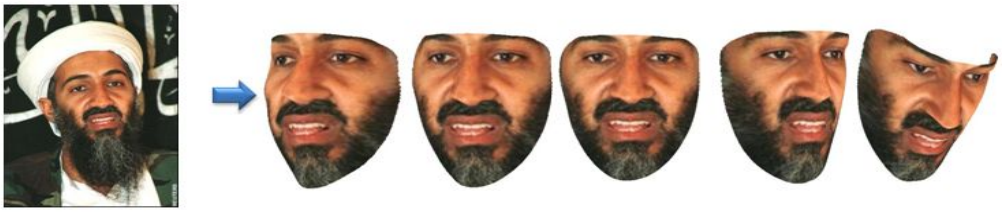
Research

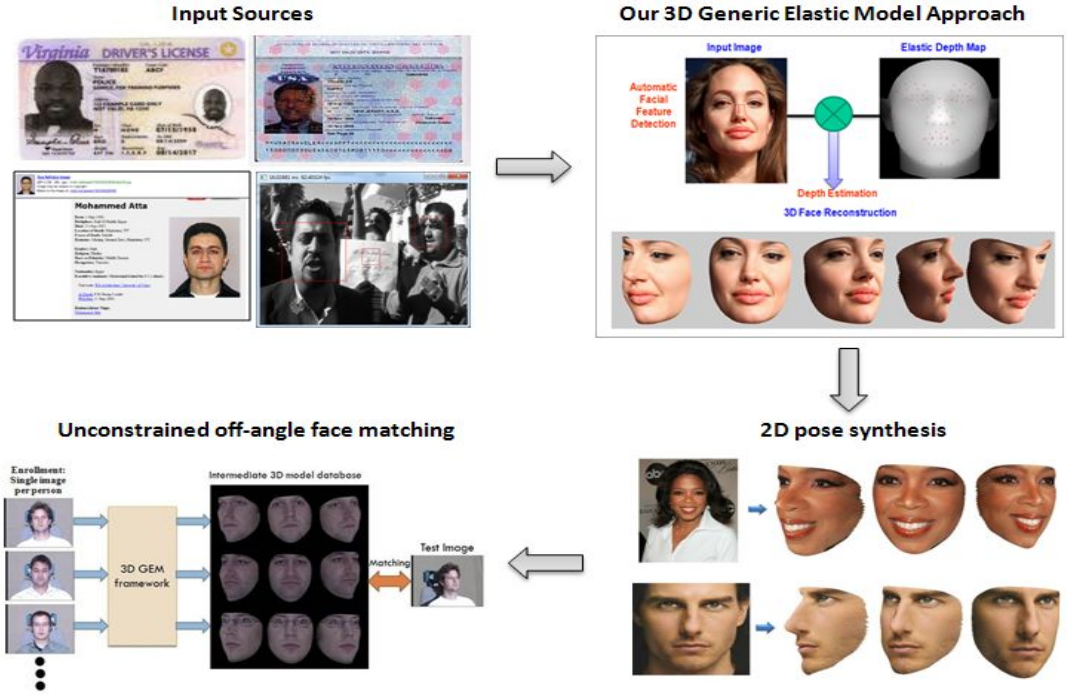
Your Pain Points	CERT Insider Threat Center Solutions	Benefits to Your Organization
How can I further improve indications and warnings of malicious behavior and detect warning signs?	• Data for non-malicious insiders is compared to malicious insiders to produce more accurate findings and guidance • Build detection algorithms (weighted rule sets)	• Automated tools produce fewer false positives – information overload is reduced • Alerts from automated tools have a higher "hit rate"
How do I stay ahead of malicious insiders who are using new and emerging technologies?	• Ongoing data collection and analysis of – new threat vectors, such as cloud computing – new data sources such as classified information and technical details regarding the cases (forensic data), trends, and forecasting • Maintain assessment framework; collect and communicate effective countermeasures discovered during assessments • Develop new countermeasures based on research and analysis	• Countermeasures and assessment are continuously updated to reflect current and emerging threats
What benchmarks can I measure myself against?	• Serve as trusted broker for collecting, aggregating, and disseminating insider threat and countermeasure information • Integrate insider threat vulnerability assessment with an enterprise-wide risk assessment process (e.g., OCTAVE, CERT-RMM)	• Ability to make better decisions based on government and industry benchmarks • Up-to-date threat and countermeasure guidance • More effective policies, standards, and mandates
How can we increase the effectiveness of insider threat researchers?	• Access to sanitized CERT database • Establish an insider threat research community of interest with facilitated access to CERT insider threat data.	• More effective defenses • More effective use of research funding • Improved information sharing among researchers
How can organizations identify similarities and differences between insider threats in the U.S. and outside the U.S.?	• Determine similarities and differences between technical and non-technical indicators and patterns of malicious insider activity in the U.S. compared to outside the U.S.	• Resulting reports and models will help international businesses and governments understand cultural influences on insider threats

Carnegie Mellon CyLab Biometrics Center Projects

Email: Marios.Savvides@ri.cmu.edu Tel: 412-980-8939

3D FACE MODELING FROM A SINGLE IMAGE

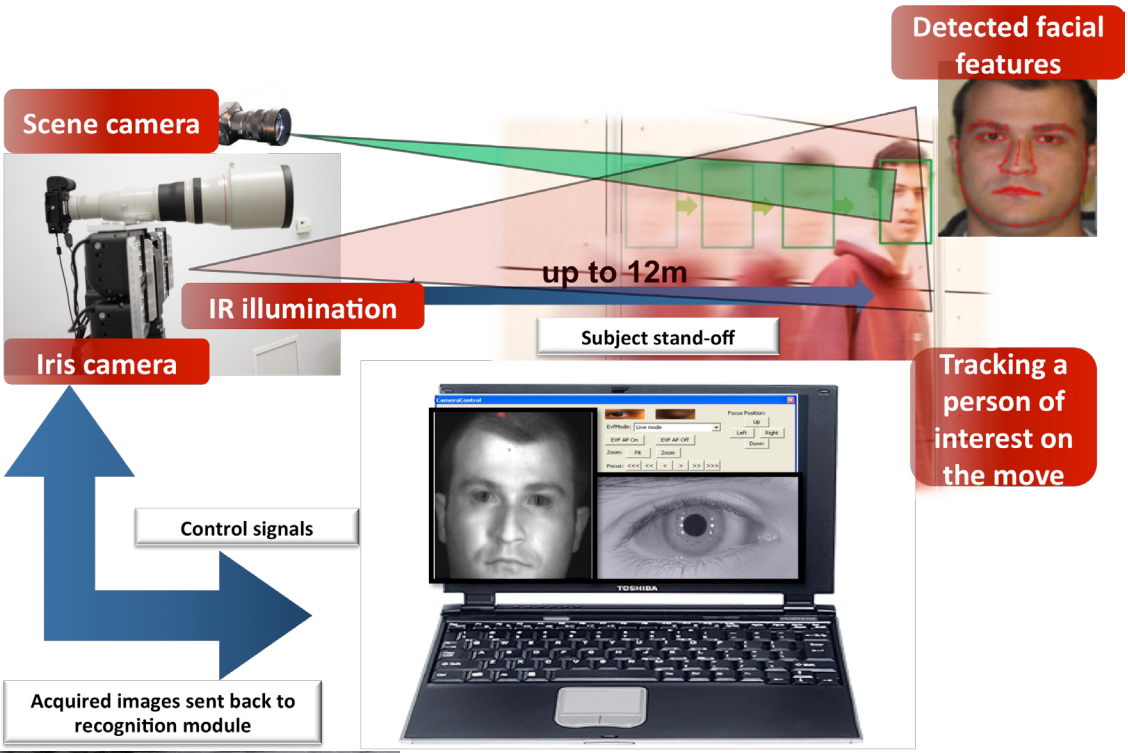


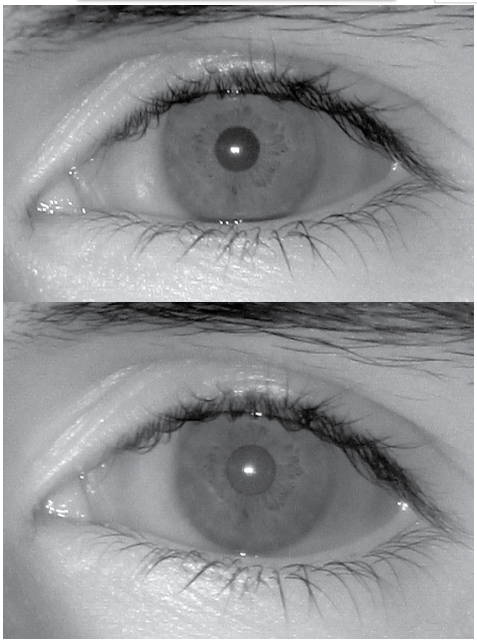


Most face recognition systems have difficulty in identifying people with off-angle non-frontal images. The CMU Cylab Biometrics Center is developing a face recognition system which handles such a wide range of angles to operate under unconstrained real world scenarios. In the enrollment stage, we generate a 3D face from a SINGLE 2D image. The depth of each 2D image is approximated from the canonical depth model while preserving the forensic information. We call this 3D reconstruction process as Generic Elastic Model (GEM) which rapidly generates 3D faces from a single 2D frontal image. In our testing stage, our 3D faces in the database rotate and align to the pose of the input test image. This off-angle face matching capability differentiates our system from other face recognition systems. Examples of 3D models using the GEM framework from a single 2D image are shown above.

VIDEO DEMOS CAN BE FOUND HERE:
http://biometrics.cylab.cmu.edu/projects/3D_from_2D/3Dall_Models.avi
http://biometrics.cylab.cmu.edu/projects/Unconstrained_Face_Matching/seinfeld.avi
http://biometrics.cylab.cmu.edu/projects/Unconstrained_Face_Matching/groundhog_day.avi

LONG RANGE IRIS RECOGNITION





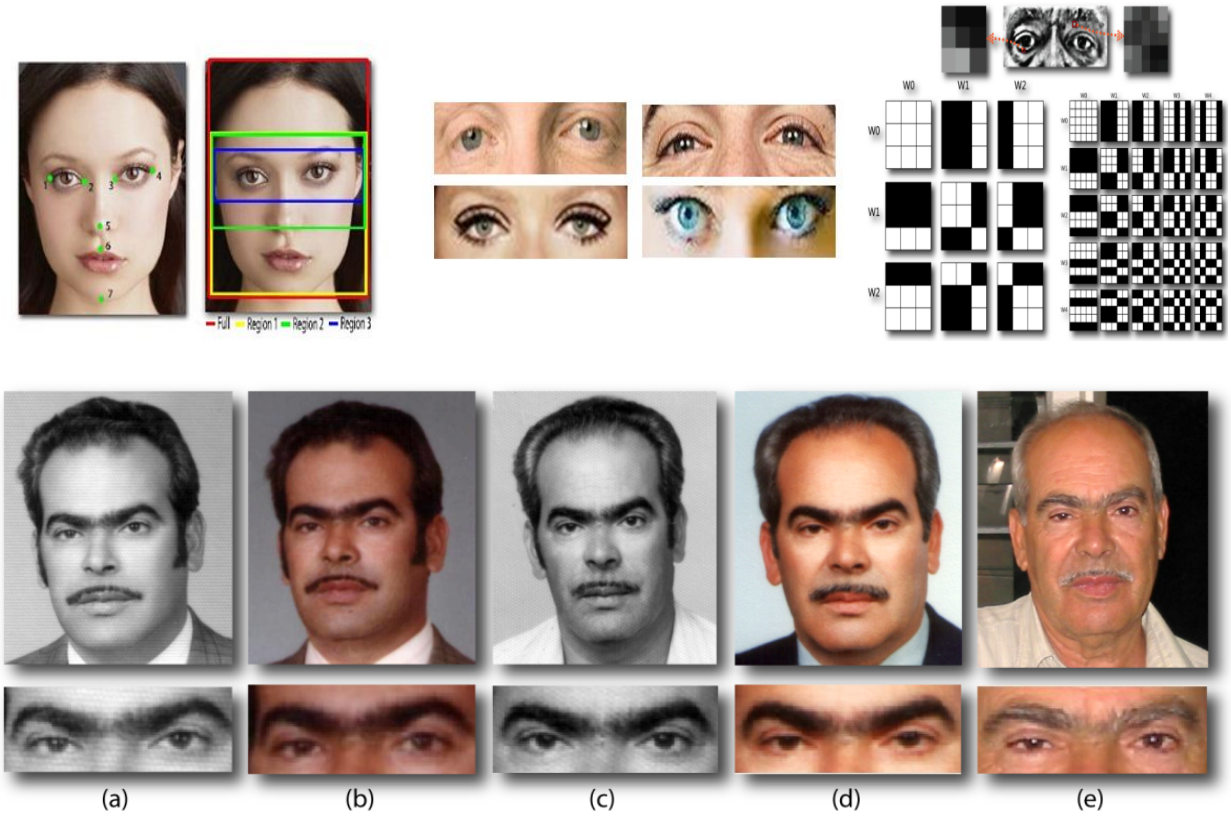
Enrollment quality iris images captured from over 9 meters away

There is a clear and present need for an inexpensive imaging system that is capable of measuring strong biometrics features from very large stand-off distances. The CMU Cylab Biometrics Center is developing a long range iris enrollment and recognition system that can be rapidly deployed. The system is based, largely, on recently released Commercial Off The Shelf (COTS) hardware, which brings down the cost. It uses infra-red illumination panels co-located with the imager to acquire iris images even during night time and low-light operation.

Our innovative design allows us to capture enrollment quality iris images at distances of upto 12 meters. The image quality is comparable to those acquired by short range systems such as the L1 PIER-T system and the LG IrisAccess systems. Also, the capture volume has been increased to 8 meters. This is a significant improvement over other long range systems which report smaller volumes of less than 3 meters.

VIDEO DEMO:
http://biometrics.cylab.cmu.edu/projects/Long_Range_Iris/Long_Range_Iris.avi

AGE INVARIANT PERIOCULAR BIOMETRICS

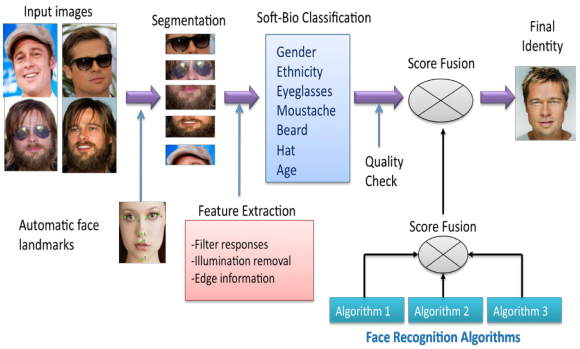


Periocular biometrics and its application for age invariant face recognition, (a) Age 31, (b) Age 40, (c) Age 46, (d) Age 61, (e) Age 69.

Classical methods in facial biometrics have experienced great success in considering the entire face region for authentication. However, these methods are highly susceptible to failure when portions of the face are occluded or obstructed. To combat this challenge, the CMU Cylab Biometrics Center is building robust biometric algorithms that use only the area surrounding the eyes, or "periocular" region as illustrated in the figure. The use of the periocular region represents a good trade-off between face recognition and iris recognition since we believe the most important features in human faces are localized around the eye regions. The Center is also investigating age invariant face recognition based on periocular biometrics. We have shown that periocular region changes the least through aging. When our developed subspace-based WHT-LBP is applied on periocular region for age invariant face recognition, we have achieved 100% rank-1 recognition rate and 98% verification rate at 0.1% false accept rate for FG-NET database evaluation.

VIDEO DEMO: http://biometrics.cylab.cmu.edu/projects/Periocular_Biometrics/Periocular Demo.avi
http://biometrics.cylab.cmu.edu/projects/Periocular_Biometrics/Periocular Demo2.avi
http://biometrics.cylab.cmu.edu/projects/Face_Aging/Age_Est.avi

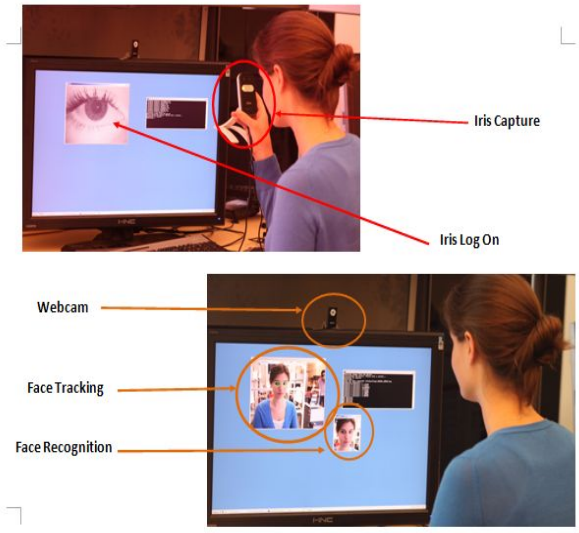
SOFT-BIOMETRICS



While humans can often recognize the same person even when changes in appearance, such as facial hair or glasses occur, many face recognition algorithms fail in attempts to match a face because they do not compensate for the differences in appearance. The Carnegie Mellon CyLab Biometrics Center aims to add intelligence to the current systems by building robust classifiers that can determine these "soft biometric" traits. Soft biometric intelligence can be integrated to improve accuracy in facial matching where match detection in conventional systems may fail due to constantly changing soft biometrics. Additionally, soft biometrics can also be used in real-time to narrow identity searches of unknown individuals. When the only a description of the subject is available, e.g. "Caucasian male with glasses and a moustache," the use of soft biometric identification can greatly and accurately assist in narrowing the search space.

VIDEO DEMO: http://biometrics.cylab.cmu.edu/projects/SoftBiometrics/SoftBiometrics_new.wmv

CONTINUOUS AUTHENTICATION



By using biometrics technologies developed at the center, we design a continuous authentication system by using a multi-model imagery such as iris and face data. Unlike conventional user identification systems, we constantly monitor and recognize a valid user while accessing a secured system. Specifically, we develop robust methods to continuously authenticate a person in front of a computer so that if the person leaves the computer will automatically lock down. If someone else not authorized is shown to try to access the computer, the system will automatically lock down. It will also lock the computer when it ceases to see a person in front of the computer. Our system continuously and periodically authenticates the user to ensure that an authorized user is using the computer.

VIDEO DEMO: http://biometrics.cylab.cmu.edu/Continuous_Authentication/CA_demo.wmv

Research, Technology, and System Solutions Program

Composing Assured Systems of Systems

The Department of Defense needs to quickly create and deploy new combinations of existing, independently developed system capabilities. The need to do so is exemplified by the Integrated Air and Missile Defense Battle Command System, which seeks to quickly combine different individual missile defense systems into a new system of systems (SoS) operational capability. The Army's Common Operating Environment has similar objectives for other types of systems.

The Research, Technology, and System Solutions Program at the Software Engineering Institute (SEI) has begun the Composing Assured Systems of Systems project to speed the fielding of such system combinations.

Challenges

Each new SoS combination presents new software integration problems, not just because of incompatible interfaces but also because of differences in operational assumptions. Even if relevant incompatibilities are removed to meet a certain mission requirement, requirements can change and new systems may be added later.

Two software engineering technology issues impede the quick integration and deployment of new combinations of systems:

- Extensive analysis and engineering are typically needed to detect and remove software incompatibilities.
- Too much time is needed to gain approval to deploy the new system.

Innovations

This project will apply two innovations to address these issues:

- Extend software product line concepts and software architecture patterns to systems of systems.
- Use assurance templates to accelerate the test and evaluation (T&E) process for new combinations of independently developed systems.

Current approaches do not support the quick development of new SoS combinations. Greater economies of development can be obtained if the composed SoS is one member of a planned capability *family* in which systems are combined according to a predefined architectural pattern.

Software product line engineering has achieved notable success. However, most of the work has been in single-organization contexts. Less well understood is the situation in which multiple organizations, each responsible for one or more core assets, cooperate to build and field the products in a product line. Plans to extend product line concepts to systems of systems must account for development efforts among multiple organizations.

Assurance templates capture a generally accepted argument that a claim about a system quality attribute is justified. The template explains a general pattern of reasoning that can be used to justify particular types of claims, including a description of what evidence is needed to support the claims.

Research Approach

Software product line concepts and software architecture patterns have both been used effectively to increase the ability to develop some kinds of systems, but these concepts have not been applied at the scale of systems of systems. Both concepts reduce the amount of engineering and analysis needed to produce a system.

In the case of product lines, the reduction occurs because a product line has been specifically engineered to produce a particular family of products. When deciding to produce a new member of the family, much of the engineering for any product in the family does not have to be redone.

Similarly, architecture patterns allow engineers to focus more efficiently on key design issues because these issues are captured in the patterns. The issues do not have to be *discovered* for each new system architecture when the architecture conforms to a known pattern because that pattern highlights what the key issues and possible solutions are.

Composing Assured Systems of Systems

The SEI Composing Assured Systems of Systems project will use SoS architecture patterns to characterize the architectures of families of mission capabilities. This project will also apply product line approaches to compose systems of systems that conform to these architecture patterns. In addition, by analyzing the commonalities and incompatibilities of potential SoS constituents, the SEI will determine how the commonalities can be exploited and the incompatibilities resolved when assembling these systems into a target SoS architecture. Although this approach has been quantifiably successful for individual software product lines, it has not previously been applied at the SoS level.

To speed up the T&E cycle for composed systems of systems, the SEI will develop assurance templates that capture the pitfalls to avoid in implementing an SoS architecture pattern correctly and will show what evidence is needed to demonstrate that the pitfalls have been successfully avoided. In addition, the template will show why evidence from previous T&E efforts can be reused in the current evaluation to reduce T&E effort without reducing confidence.

This use of templates is new in that assurance templates have not previously been developed for SoS assurance claims and have not previously been linked with issues raised (and avoided) by using an associated architecture pattern. In addition, the product line approach lends itself to the notion of standardized assurance arguments (reusable assurance assets) associated with the product line scope and the process used for composing a product from its constituents.

Objectives

The Composing Assured Systems of Systems project will help engineers develop new SoS capabilities for the warfighter more quickly and cheaply. Using a product line approach can greatly reduce the time required to integrate a new combination of existing systems. In turn, this will reduce the time needed to gain approval to deploy the new system combination.

Related Web Sites

www.sei.cmu.edu/ productlines/
www.sei.cmu.edu/dependability/tools/assurancecase/index.cfm

For General Information

For information about the SEI and its products and services, contact
Customer Relations
Phone: 412-268-5800
FAX: 412-268-6257
customer-relations@sei.cmu.edu
www.sei.cmu.edu

Research, Technology, and System Solutions Program

Edge-Enabled Tactical Systems

A team of first responders searches a metropolitan area hours after a devastating earthquake. The responders carry mobile phones loaded with an app to collect, share, and catalogue information related to their mission. They use the app to record the area affected on a map, the extent of damage, and the address of each residence they search. They also note GPS coordinates, obtained directly from a sensor in the phone, to record areas searched. The areas searched can then be shared with other responders, allowing the whole team to get a better picture of the situation. The responders soon realize, however, that they need to capture more information. So, using an intuitive programming interface, they add a "casualties" field to the app. They also configure the app to acquire the number of known residents for each address they search from a database in the command center. Having made these changes in the field, the responders proceed with greater accuracy and efficiency.

This is the vision of the technical staff of the Research, Technology, and System Solutions Program at the Software Engineering Institute (SEI). The SEI sees great potential in providing user-controlled system adaptation to first responders, warfighters, and others working with handheld devices in tactical environments at the edge, or periphery, of the network.

Challenges

According to recently deployed soldiers, dismounted warfighters have access to only limited information about the enemy, noncombatant population, terrain, and weather—even when this information is available elsewhere in the enterprise. These are some of the challenges they face:

- Software delivered to warfighters does not keep pace with changing missions.
- Warfighters cannot get the relevant information they need at the time they need it.
- The closer that warfighters get to combat, the fewer resources they have available.

Innovations

The SEI is conducting the Edge-Enabled Tactical Systems project to improve the quality and relevance of warfighter information in three ways:

- **User-controlled system adaptation at the edge:** Deployed soldiers can modify apps while architectural strategies ensure that modifications stay within prescribed bounds.
- **Information superiority at the edge:** The software will integrate contextual information from individual soldiers, nearby soldiers operating as part of a unit, and remote systems.
- **Resource optimization for mobile platforms at the edge:** Algorithms will address resource limitations by optimizing energy and CPU consumption among both individual handhelds and nearby peer devices.

Research Approach

Dismounted warfighters involved in patrols and other operations at the tactical edge have often been the last to benefit from systems and software to improve situational awareness. These warfighters typically have access to very limited bandwidth—sometimes only voice radio—and cannot access existing information that would improve their effectiveness.

The goal of the SEI Edge-Enabled Tactical Systems project is to improve the quality and relevance of information available to dismounted (edge) warfighters so that applications running on handheld devices can be readily customized by warfighters to support new missions; the information they receive will be more consistent with and useful for the current mission; and they will consume fewer battery, computation, and bandwidth resources when performing their missions.

The SEI will develop end-user strategies to support user-controlled adaptation of apps on handheld devices. One such strategy, *natural programming*, will be piloted to gather requirements for end-user adaptation and the user interface.[1] Natural programming focuses on how people perform their tasks and then designs languages and environments around people's natural tendencies. This provides a warfighter-specific approach for enabling the types of modifications that are most

appropriate for achieving effectiveness in the field.

Warfighters also require a rich model context containing high-value information. The SEI will create a model that combines information from the warfighter, the warfighter's unit, and the enterprise as a whole. The model will synchronize across peers and extend the sources of contextual information beyond location and time.

The value of smartphones in tactical environments will in part be determined by how long they function before the battery is drained. The SEI's approach will also focus on group battery optimization, which applies context information for the individual and unit to optimize battery usage across a squad of soldiers in the field.

Objectives

User-controlled system adaptation at the edge will speed up delivery and reduce costs by supporting tailoring in the field. The capability will validate warfighter changes by providing feedback regarding impact, firewall changed components, and perform real-time monitoring to ensure that the modified parts of the system do not exceed constraints.

Information superiority at the edge will apply advanced strategies for human-computer interaction that reduce the need for error-prone verbal transmission, ensure that only relevant information is received, and prevent information overload.

Resource optimization for mobile platforms at the edge will preserve warfighter resources by extending individual and unit battery life and computational capability.

Related Web Site

www.sei.cmu.edu/sos/research/mobilecomputing/Edge-Enabled-Tactical-Systems.cfm

For General Information

For information about the SEI and its products and services, contact
Customer Relations
Phone: 412-268-5800
FAX: 412-268-6257
customer-relations@sei.cmu.edu
www.sei.cmu.edu

[1] Myers, B. A., et al. "More Natural End-User Software Engineering," 30–34. *Proceedings of the 4th International Workshop on End-User Software Engineering*. ACM, 2008.

Research, Technology, and System Solutions Program

High-Confidence Cyber-Physical System

To be successful in modern warfare, defense systems demand an increasing number of capabilities. A large number of these capabilities are based on software. When these capabilities interact with physical processes in tight loops, such as the control of the aerodynamics of an aircraft, they fall into the realm of cyber-physical systems (CPS). These systems need to execute correctly and in a timely fashion to keep the physical processes under control, for example, to enable a stable flight.

CPS play an increasingly crucial role in delivering mission-critical capability to the Department of Defense (DoD). They are critical to the safe and reliable operation of virtually all missions. In many cases, such as a modern fighter jet or unmanned aerial vehicle (UAV), the entire system is essentially a complex CPS. The Research, Technology, and System Solutions Program at the Software Engineering Institute (SEI) aims to enable the DoD to maintain its competitive advantage through cost-effective delivery of reliable mission-critical capability via high-confidence CPS.

Challenges

A recent National Research Council report noted that CPS "are increasingly critical in defense applications of all kinds and at all levels of scale."[1] Moreover, as the DoD's reliance on CPS-driven capability has increased, so has the cost of failure of CPS. Defense systems safeguard human lives and national assets. Delay in delivering CPS-driven mission-critical capability must be minimized. The SEI will concentrate on two specific challenges to achieve this goal:

- Current functional algorithms for real-time software produce too many false warnings and have hindering time and memory limits.
- Current timing analysis leads to low CPU utilization, forcing designers to limit capabilities to ensure that real-time tasks meet their deadlines.

Innovations

The High-Confidence CPS project will address these challenges by focusing on functional correctness and timing correctness. The SEI approach involves two innovations:

- **Static Analysis of Real-Time Software (START):** The key technical objective is to balance precision with scalability. This requires developing analyses that can handle real-time embedded software of realistic complexity while yielding few false warnings.
- **Resource allocation for multi-core CPUs with nonuniform memory access:** The technical objective of this task is to optimally schedule access to a shared resource by different tasks and minimize overall task latency. This requires novel scheduling algorithms that minimize delays in the critical execution paths of each task.

Research Approach

New characteristics of defense CPS systems and processor technology have created new technical challenges for both functional verification and validation (V&V) as well as resource allocation and scheduling theory.

- **Growing use of small, autonomous defense vehicles (e.g., UAVs) demands more capabilities in a smaller number of processors.** Examples of these capabilities include autonomous route planning, obstacle avoidance, and surveillance-video processing. Increasing capabilities leads to more complex software, which in turn increases functional V&V cost. In particular, traditional testing-based

approaches become prohibitively expensive.

- **Improvement in processor technology shifted from faster processors to processors that execute more instructions in parallel (multi-cores).** To take advantage of this new technology, it is necessary to increase the number of processor cores (known as multi-core processors) that can execute multiple functions in parallel. Doing so demands a departure from traditional scheduling schemes in which only one core had to be scheduled to run a single sequence of instructions (a single thread of instructions). In contrast, to use multi-core processors effectively, it becomes necessary to schedule multiple sequences of instructions running in parallel (multiple threads) on multiple cores.

Early experiments in multi-core processors highlighted a new complication: the execution time of a function in one core can be severely affected if another (unrelated) function is executed in another core of the processor. Even though instructions can execute in parallel in different cores, their access to shared memory needs to be serialized, and hence one can delay the other. Such slowdowns have prevented defense systems from leveraging multi-core processors. Sometimes engineers employ extreme strategies such as disabling all but one core to avoid the inter-core interference. Thus, as multi-core processors need to share common memory, the initial speed up gained by adding cores to a processor can also be rapidly lost.

Static analysis research focuses on delivering precise and scalable function V&V capabilities. The SEI solution will be to limit the exploration of infeasible paths during functional verification by leveraging scheduling constraints. Consider tasks scheduled by priority—a common situation in avionics software. In this setting, the SEI will develop functional-verification algorithms that incorporate techniques to deal with infeasibility due to illegal preemptions and infeasibility due to too many preemptions. Cumulatively, the two techniques will reduce the number of executions explored and the number of false warnings generated. Consequently, verification will take less time and memory.

Resource allocation research will focus on reducing the completion time of real-time multi-threaded tasks. This reduction will be based on the assignment and scheduling of shared resources (e.g., memory and memory bandwidth) in a way that minimizes the impact of the contention for common resources in the critical path of the tasks.

Objectives

The High-Confidence CPS program will help reduce testing costs. By applying functional analysis to designs and high-level artifacts, engineers can detect faults earlier. Additionally, increased processing capacity will be leveraged to deliver increased mission capability. For example, UAVs can incorporate more functionality without increasing their form factor. This research project will also advance the state of the art in the validation, verification, and analysis of CPSs, all of which will enable producibility improvements.

For General Information

For information about the SEI and its products and services, contact
Customer Relations
Phone: 412-268-5800
FAX: 412-268-6257
customer-relations@sei.cmu.edu
www.sei.cmu.edu

[1] Committee for Advancing Software-Intensive Systems Producibility & the National Research Council. *Critical Code: Software Producibility for Defense*. National Academies Press, 2010.

Research, Technology, and System Solutions Program

Socio-Adaptive Systems

Due to reports of insurgent activity, a platoon must sweep a village for small arms caches. A small number of unmanned aerial vehicles (UAVs) will provide video surveillance of the village center. These UAVs transmit analog video feeds to ground stations, where they are digitized and forwarded to the troops. Four squads will perform the sweep. During mission planning, the squad leaders request surveillance data to assist in their mission roles. Some squad leaders are overly cautious and have exaggerated the importance of such data in past missions. Network Operations Center staff judge network capacity to be insufficient to stream surveillance data to all four squads. How will they allocate network resources whose capacity changes in a manner that optimizes the likelihood of mission success, while being attentive to the possibility of overstated need?

The Research, Technology, and System Solutions Program at the Software Engineering Institute (SEI) created the Socio-Adaptive Systems project to help enable effective, mission-aware use and adaptation of tactical resources. A direct consequence of achieving this objective is that scarce tactical network capacity will automatically, continuously, and effectively be allocated to warfighters based on their own accurately reported needs. The SEI aims to establish a new approach for designing adaptive socio-technical systems wherein people, networks, and computer applications can locally decide how to respond when the demand for resources outstrips supply, while guaranteeing the best global use of whatever capacity is available.

Challenges

This research combines the adaptability of human social institutions, in particular those based in market institutions, with automated network-resource optimization. On the human side, U.S. warfighters are unmatched in their training and ability to act independently and to make complex decisions when confronted with unexpected circumstances. But ever faster operational tempos and the vastly expanded importance of digitally networked resources, combined with a proliferation of new uses for those resources, require substantial automation of resource allocation and optimization procedures.

Significant new challenges must be addressed to create the desired socio-adaptive combination:

- Overstated needs continually affect resource allocation.
- Commanders do not have access to timely, reliable estimates of network capacity.

Innovations

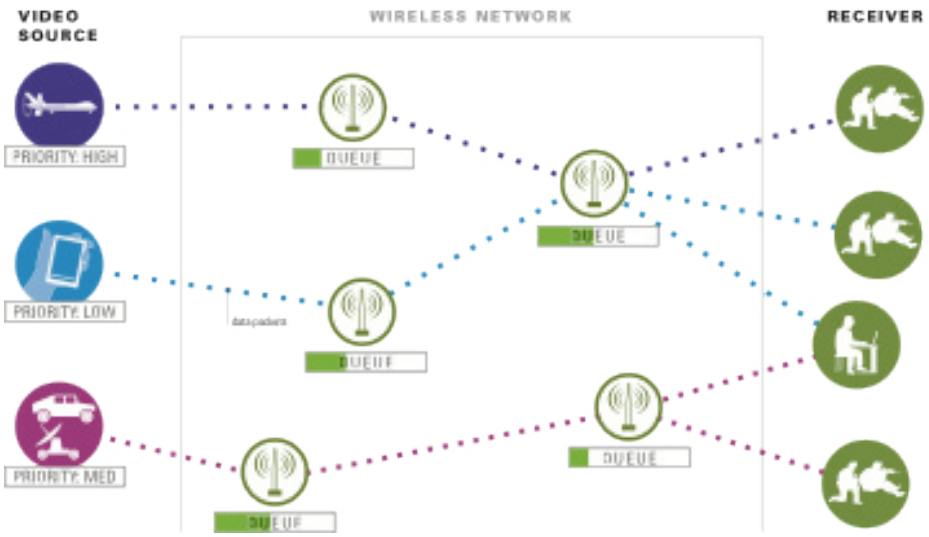
In actual operations, commanders face decisions involving more resources and operational consequences than those in the guiding scenario. The SEI will focus on two interrelated tasks to address the challenges of allocating scarce network resources in environments of uncertainty and change:

- Use computational mechanism design (CMD) to elicit changing mission needs and compute an optimal allocation of resources.
- Use decentralized quality-of-service (QoS) optimization to optimally respond to changes in tactical resource capacity.

Research Approach

The SEI applies microeconomic foundations known as CMD to address the decentralized and dynamic nature of network resource allocation in a tactical setting. There is significant literature on using incentive-compatible market mechanisms (i.e., mechanisms that cause market participants to truthfully reveal relevant information) for allocating computational resources, but little work has been done to address the dynamics and uncertainty that typify tactical operations. SEI research builds on and extends prior work by generalizing promising mechanisms that model the effects of uncertainty on current and future allocation decisions.

The SEI will develop a distributed version of the QoS resource allocation model (Q-RAM)[1] to allocate tactical resources to applications requiring those resources.



Distributed Q-RAM (D-Q-RAM) is novel in that it does not require a centralized aggregator of application QoS information, nor does it require explicit knowledge of the capacity of tactical resources. D-Q-RAM provides a vehicle for expressing mission needs in an incremental way, wherein different levels of QoS are associated with expressions of mission utility or value. Given that each application expresses its utility for various levels of QoS, D-Q-RAM provides a way to optimally allocate tactical resources. CMD will rely on D-Q-RAM to compute an optimal allocation based on warfighter input.

Unlike previous work, the SEI approach makes explicit and quantifiable the relation between warfighter needs *as they perceive these needs* and the ability of the tactical network to satisfy these needs. Further, this approach provides adaptation mechanisms that allow network performance to degrade gracefully in a way that maximizes mission value. Finally, although both tasks focus on allocating scarce network capacity, the results of this work can be generalized to other scarce tactical resources, such as UAVs or cloud capacity. Moreover, this overall approach is largely agnostic about the underlying mobile ad hoc network protocol and can therefore be combined with a variety of networking infrastructures.

Objectives

This capability will improve current practice in several ways:

- **Incentive-compatible allocation procedures:** The best outcome for each warfighter is obtained when warfighters report their *true* needs. Warfighters will be able to continuously report their changing needs for digital resources without having to exaggerate or otherwise speculate on how their reports will influence allocation decisions.
- **Effective bandwidth allocation:** The proliferation of digital resources, the growing diversity of their uses in tactical networked operations, and the quickened tempo of these operations demand a high degree of automation in the management of scarce resources. This capability will significantly reduce reliance on manual intervention to deliver reliable network capabilities where it is most needed, and in time to meet those needs.
- **Gracefully degrading QoS when network demand outstrips capacity and automatically recovering when capacity becomes available:** SEI research allows the network infrastructure and the applications it supports to agree on a range of actions that the application can take to exploit increased network capacity and to accommodate reduced network capacity.

For General Information

For information about the SEI and its products and services, contact
Customer Relations
Phone: 412-268-5800
FAX: 412-268-6257
customer-relations@sei.cmu.edu
www.sei.cmu.edu

[1] Lee, C., Lehoczky, J., Rajkumar, R., & Hansen, J. "A Scalable Solution to the Multi-Resource QoS Problem," 315–326. *Proceedings of the 20th IEEE Real-Time Systems Symposium.* IEEE Computer Society Press, 1999.

Research, Technology, and System Solutions Program

Value-Driven Incremental Development

"Get me an 80% solution NOW rather than a 100% solution two years from now and help me innovate in the field."

—Honorable Zachary Lemnios, Assistant Secretary of Defense for Research and Engineering[1]

The Department of Defense (DoD) increasingly must respond to rapidly changing and less predictable threats. The objective of the Value-Driven Incremental Development project is to create quantitative engineering techniques to support rapid delivery of high-value, high-quality software capabilities to the warfighter. This research also tackles the underlying challenge to release smaller increments of features; slow, massive software release processes are no longer satisfactory. The payoff for achieving this objective is that program offices will have greater ability to get warfighters the features they need most, when they need them, while balancing speed-of-delivery, quality, value, and cost tradeoffs.

Challenges

Rapid fielding of high-quality capabilities is a key goal for the DoD. However, it typically takes years from identification of an operational need before a solution is deployed. There are programmatic and process barriers to achieving this rapid delivery, but there are technical barriers as well:

- Program officers and developers lack engineering techniques to make economically informed design decisions for quicker delivery of capabilities.
- The lack of a way to evaluate the effectiveness of assurance techniques makes it difficult to determine which to eliminate to allow for faster deployment at a lower cost.

Innovations

The Research, Technology, and System Solutions Program at the Software Engineering Institute (SEI) is conducting a research and development project in value-driven incremental development. The SEI will create an incremental development approach riveted in the structure of a system, supported by essential runtime quality attributes, and offering the assurance necessary to support rapid deployment of capabilities. The SEI's contributions will advance the state of the art in several ways:

- Ability to deliver capabilities incrementally while maintaining desired runtime quality attributes.
- Ability to make informed cost-benefit decisions for delivering capabilities incrementally in an agile environment.
- Ability to provide cost-effective assurance at each increment by focusing on the value of assurance activities.

Research Approach

A program office trying to plan rapid delivery increments has very little insight into the features to be fielded in the early increments. Indeed, these needs often change before the scheduled fielding. This results in the lack of delivery of any features to the field early on. Even if a development team had these insights, systems are not typically architected with sufficient flexibility to integrate any new feature rapidly while maintaining the quality of the rest of the system. Critical static and runtime dependencies that can slow development of new features may not be adequately identified. Even if they are, the features may require a lengthy certification and recertification.

The Value-Driven Incremental Development project will create quality attribute-based analysis models to guide incremental development by discovering runtime dependencies early in the life cycle. This will allow software developers to understand the impact of new capabilities and how they affect future development.

This work is innovative in two ways: (1) It will enable engineers to monitor the developmental "health" of a system through observing the quality of its architecture over time so they can understand the implications of the decisions they make or defer. (2) The work will enable engineers to develop a capability rapidly while maintaining the integrity of the system.

The SEI will also create an economic framework to view development progress in terms of both costs incurred and value produced. This framework will measure system value based on both capabilities and utility delivered through overall system quality, with flexibility created for the future.

Research, Technology, and System Solutions Program

Value-Driven Incremental Development

This work is innovative in providing information about the strategic value of early deployment of a capability with suboptimal quality and an understanding of the cost and benefit tradeoffs in an agile context. How much quality is enough? The work will help engineers decide which capabilities, or which parts of them, to implement.

The SEI will use probabilistic models of evidence borrowed from the legal, philosophy, and mathematics communities to understand how to assign confidence levels to particular pieces of evidence. The SEI will also use inference techniques and assurance cases to determine how the confidence in individual pieces of evidence rolls up into confidence in the entire incrementally developed system. The work will help engineers contribute to rapid development by allowing some activities to be eliminated while providing high-confidence validation in a cost-effective manner.

Objectives

This work will lower technical barriers to the rapid development and fielding of DoD systems. Extending current incremental-development techniques will provide several benefits:

- **Faster delivery of capability to the warfighter, while preserving required system-runtime qualities:** By emphasizing preservation of runtime qualities in a system rather than focusing exclusively on functionality, this research will overcome a key limitation to the application of Agile methods to large systems.
- **A means of prioritizing the capabilities to be delivered by value:** Faster delivery of capabilities is a hollow concept unless the capabilities deliver sufficient value. This research will develop the means to go beyond traditional qualitative priority setting by stakeholders.
- **Justifiable confidence in incrementally delivered capability:** Assurance techniques are a central aspect of incremental development and often require the most time to perform. Selecting the most effective assurance techniques will provide necessary confidence in the delivered capability while reducing development time.

For General Information

For information about the SEI and its products and services, contact
Customer Relations
Phone: 412-268-5800
FAX: 412-268-6257
customer-relations@sei.cmu.edu
www.sei.cmu.edu

[1] Science and Technology Keynote Remarks as prepared by the Honorable Zachary J. Lemnios, Director, Defense Research and Engineering, Department of Defense, to the Defense Technology and Requirements Conference, sponsored by Aviation Week, Washington, D.C., February 17, 2010.

A New Approach for Handheld Devices in the Military

By Edwin Morris, Senior Member of the Technical Staff, Research Technology and System Solutions

Edwin Morris Many people today carry handheld computing devices to support their business, entertainment, and social needs in commercial networks. The Department of Defense (DoD) is increasingly interested in having soldiers carry handheld computing devices to support their mission needs in tactical networks. Not surprisingly, however, conventional handheld computing devices (such as iPhone or Android smartphones) for commercial networks differ in significant ways from handheld devices for tactical networks. For example, conventional devices and the software that runs on them do not provide the capabilities and security needed by military devices, nor are they configured to work over DoD tactical networks with severe bandwidth limitations and stringent transmission security requirements. This post describes exploratory research we are conducting at the SEI to (1) create software that allows soldiers to access information on a handheld device and (2) program the software to tailor the information for a given mission or situation.

To motivate the need for tactical handheld devices, imagine a U.S. soldier on patrol, deployed abroad, and walking into an unfamiliar village. Many pieces of information would be useful to that soldier in that situation. For example, it would be useful to know who the village elders are and to have pictures to identify them. It would also be useful to access information about previous IED attacks or reports detailing the results of other contact that soldiers have had with villagers, and whether any friendly villagers speak English. We face the following challenges when creating software for tactical handheld computing devices that can provide this information:

Developing applications that can support the full range of military missions. In recent years, soldiers have provided humanitarian assistance to victims of natural disasters in Haiti and countries in Asia, patrolled our country's borders, protected global waterways from piracy, and performed many types of military operations in Iraq and Afghanistan. These missions are sufficiently diverse that a one-size-fits-all software solution is not practical. For example, consider the different goals of clearing a route in a combat zone versus delivering humanitarian supplies in a relief effort or the different information required to protect from IED attacks versus treat a critically ill child.

Not only is different information required, but also the rules for sharing it can vary. In a combat environment, security concerns require limiting access, while information in a relief mission may be shareable with non-governmental organizations responding to the crisis.

Processing large amounts of data available through the rapid computerization and internetworking of various military missions. For example, the military employs hundreds of unmanned aerial vehicles (UAVs) that generate large amounts of data. There are also increases in the number of sensors, such as auditory, biological, chemical, and nuclear, that are network-enabled. All the data generated from these devices makes it hard to pinpoint the right information for a given mission and situation.

Our goal is to ensure the capabilities provided on tactical handheld computing devices are flexible enough to allow solders to control the amount and type of data that they receive and adaptive enough to meet the needs of particular missions. To achieve this goal we are exploring the integration of end-user programming techniques, active data filtering and formatting, and confidence-building strategies. End-user programming techniques enable soldiers to program software on tactical handheld devices without requiring them to be professional software developers. Filtering incoming information and displaying it in intuitive formats helps avoid inundating soldiers on patrol with too much data. Confidence-building strategies promote trust that applications programmed by soldiers work correctly and safely. We are currently developing software for Android devices, but the fundamental concepts are applicable to other mobile platforms as well.

A key concern is designing software that has an intuitive and simple to use interface since the soldiers customizing these capabilities are not programmers; they are war fighters. The software we build must therefore help them readily find and assemble the types of information they need. It should reduce the soldier's workload by filling in (auto-complete) as much information for the soldier as possible. The software should require soldiers to learn only a few different types of screens (for example, screens for entering data and for establishing filters should be substantially the same.) In addition, confidence-building feedback should be integrated into the interface so that soldiers are sure that what they build will work and are informed early if it will not.

Our work also focuses on ensuring that the information—whether from central command or a local unit—makes its way quickly and efficiently to the handheld computing device used by soldiers. For example, user-programmable data filtering allows soldiers to specify what information is important. Likewise, optimized protocol implementations ensure this information is exchanged quickly.

Last year, we conducted a research project that involved taking a service-oriented architecture (SOA) approach to provide real time situational awareness data to Android smartphones. We worked with soldiers through the Naval Post-Graduate School's Center for Network Innovation and Experimentation (CENETIX) to test our applications. They told us what capabilities they need, and what did not work. These collaborations tie our work firmly into both the research and military communities and keep us focused on providing a useful and cutting-edge capability. In addition to continuing our collaboration with CENETIX, we are working with Dr. Brad Myers of the Carnegie Mellon University Human Computer Interaction Institute. Dr. Myers is helping us define an appropriate interface for soldiers to use the handheld software in the challenging situations they face.

This is an ongoing research project and I will be providing periodic updates on its progress throughout the year.

Related Web Sites

http://blog.sei.cmu.edu/post.cfm/a-new-approach-for-handheld-devices-in-the-military

For General Information

For information about the SEI and its products and services, contact
Customer Relations
Phone: 412-268-5800
FAX: 412-268-6257
customer-relations@sei.cmu.edu
www.sei.cmu.edu

07/28/2011

Edge-Enabled Tactical Systems

Operational images built and sent via handheld devices aid soldiers in the field.

The Software Engineering Institute (SEI) is a federally funded research and development center at Carnegie Mellon University. The SEI works with defense and government organizations, industry, and academia to improve software-reliant systems. As part of its mission, the SEI funds several internal research and development (IRAD) projects each year. This year, the SEI is funding the Edge-Enabled Tactical Systems IRAD.

The objective of this IRAD is to enable boots-on-the-ground warfighters to build mission-specific operational pictures on handheld smartphones and tablet computers. These devices are rapidly entering service through initiatives such as "Connecting Soldiers with Digital Applications." The SEI's goal is to improve warfighter effectiveness and safety by bringing tailorable and real-time situational awareness to the smallest tactical unit.

The challenge for the Edge-Enabled Tactical Systems IRAD is to identify and implement a strategy that supports warfighter-directed tailoring of operational pictures provided on handheld devices. Achieving this capacity involves filtering large volumes of data to reduce unnecessary clutter and increase the relevance of data that soldiers receive in the field. Warfighter control over what information is displayed and how it is displayed is also essential. Key to success is enabling capabilities that allow warfighters to adapt operational pictures to support the wide range of missions that they undertake—from humanitarian to civil support to warfighting—and doing it all on the handheld devices that all soldiers will carry with them in the future.

As part of the Edge-Enabled Tactical Systems IRAD, the SEI would like to interview recently deployed individuals and groups of soldiers, and other experts in the field, who can help identify critical warfighter information needs and how these needs change based on the mission. This input will help the SEI provide the right information in the right format for use by warfighters. Interviews can be conducted via telephone or in person.

If you are interested in assisting in this effort, please call

Ed Morris (ejm@sei.cmu.edu)

Software Engineering Institute,
Carnegie Mellon University

412 268-5754

For General Information

For information about the SEI and its products and services, contact
Customer Relations
Phone: 412-268-5800
FAX: 412-268-6257
info@sei.cmu.edu
www.sei.cmu.edu

Software Engineering Institute | Carnegie Mellon

Investigating the Feasibility of Service-Oriented Architecture with Handheld Computing Devices in Tactical Environments

Problem

Through increasingly sophisticated but often special-purposed devices, warfighters on patrol are now or will be soon linked into their communications network as information gatherers and users and as recipients of situational awareness data. Warfighters—as well as emergency first responders and others operating in similar resource-poor environments—need reliable, real-time access to mission-critical information without the addition of (and weight of) multiple, special-purpose devices.

Dan Plakosh
dplakosh@sei.cmu.edu
412.268.7197

Soumya Simanta
ssimanta@sei.cmu.edu
412.268.7602

Ed Morris
ejm@sei.cmu.edu
412.268.5754

Bill Anderson
wba@sei.cmu.edu
412.268.5386

Joe Seibel
jseibel@sei.cmu.edu
412.268.7736

For More Information

SEI Customer Relations
info@sei.cmu.edu
412.268.5800
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213-3890
www.sei.cmu.edu

Approach

Carnegie Mellon University® Software Engineering Institute (SEI) researchers and others have recognized that the combination of two available technologies might place mobile software applications in the hands of warfighters in the battlefield.

These researchers are investigating whether characteristics of the service-oriented architecture (SOA) paradigm and commercial handheld computing technology can be applied to tactical environments. The SOA paradigm provides a standardized interface format for the exchange of information, simplifying platform-to-platform interoperability. Also, commercial handheld computing technology, in the form of smartphones, offers portability, light weight, and support for voice, text, image, and video data.

SEI researchers are investigating

- an emerging architectural paradigm that employs lightweight, handheld devices to provide situational awareness information to edge users such as soldiers and first responders and allows them to provide information back to base
- whether service-oriented approaches employing Extensible Markup Language (XML) and SOAP are viable in light of the potential limitations in tactical environments, especially resource scarcity on smartphones and low network bandwidth
- whether reasonable quality of service for performance and security could be delivered on commercial handheld devices using existing service-oriented principles and open source off-the-shelf implementations

Experiment Design

The SEI team implemented a series of prototypes to test the viability of using service-orientation (via SOAP-based web services) and mobile handheld technologies (Android mobile computing stack) to access information from tactical assets, including unmanned aerial vehicles (UAVs), and to use this information to enhance the situational awareness of warfighters.

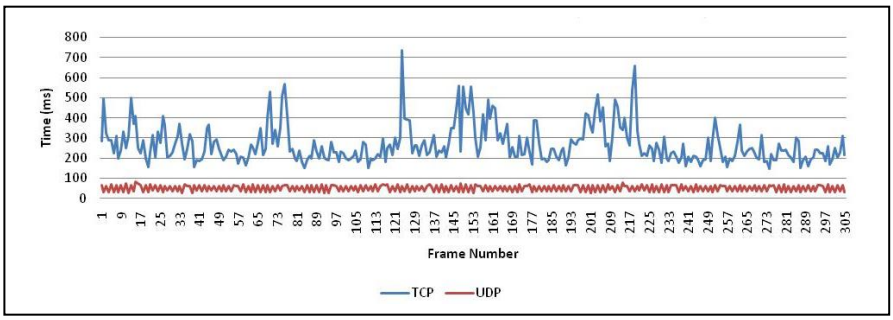
The prototypes were developed in the SEI RTSS[1] Concept Lab environment in Pittsburgh, Pennsylvania using existing technology, standards, and open source implementations. The prototypes were tested at the USSOCOM-NPS Field Experimentation Cooperative Capabilities Based Experimentation (CBE) lab at Camp Roberts, California.

1 RTSS is the Research, Technology, and System Solutions Program.

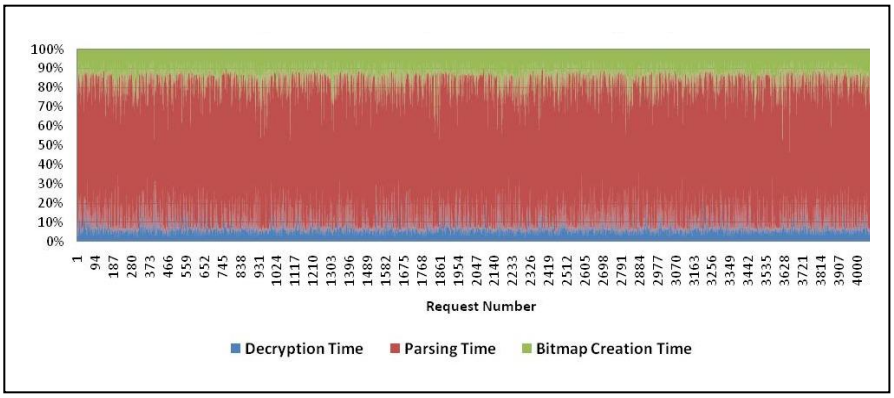
Investigating the Feasibility of Service-Oriented Architecture with Handheld Computing Devices in Tactical Environments

From the experiments, the team gathered performance data on the prototypes concerning

- overhead incurred by the transformation of data from tactical assets (e.g., sensors, UAVs, etc.) into SOAP messages and the parsing and decoding of these messages by the smartphone
- comparison of the performance of SOAP messaging over TCP and UDP protocols to provide real-time video feeds to a smartphone
- overhead involved in smartphone to smartphone SOAP messaging using an intermediary for routing
- overhead of support for network- and application-level security appropriate to the target environment



UDP and TCP performance: The blue graph represents the inter-arrival times under high network load conditions for MJPEG frames when using the TCP transport strategy; the red graph represents those times using UDP. In general, the UDP strategy demonstrated more consistent arrival and reduced lag between frames.



Smartphone to smartphone performance: The blue area represents the percentage of time required to decrypt a message that encodes a video image on the smartphone; red represents the time to parse the SOAP/XML message, and green represents the time to create the bitmap for rendering on the phone's screen. The SOAP/XML parsing time dominates the other times, requiring more than 8 times the decryption time, and more than 5 times the bitmap creation time.

Analysis

A subset of SOA is practical in tactical environments—performance of video feeds (using SOAP-based messaging) displayed on the smartphone is comparable (visually) to video feeds displayed on standard desktop machines. However, the use of SOAP leads to large message sizes that may be problematic in networks with highly constrained bandwidth. In addition, to make SOA practical, the SEI team made atypical SOA choices, including the use of UDP as a transport layer protocol rather than the TCP/HTTP combination.

Also, **the smartphone (Google's Nexus One) exceeded expectations**—it is roughly as powerful as a circa 2000 desktop machine and provides a sophisticated software development platform.

Next Steps

The experiments identified other engineering issues to consider in future work, including

- improving performance through support of *on demand* messaging
- implementing a reliability layer on top of UDP to address issues that arise when packets carrying text messages are lost
- splitting messages across packets to support higher resolution images (UDP packet size limit is 64K)
- evaluating limitations and incompatibilities of SOAP implementations for smartphones and Windows computers

The Software Engineering Institute (SEI) is a federally funded research and development center sponsored by the U.S. Department of Defense and operated by Carnegie Mellon University.

Cloud Computing for the Battlefield

By Grace Lewis, Senior Member of the Technical Staff, Research, Technology, and System Solutions Program

The Department of Defense (DoD) is increasingly interested in having soldiers carry handheld mobile computing devices to support their mission needs. Soldiers can use handheld devices to help with various tasks, such as speech and image recognition, natural language processing, decision-making and mission planning. Three challenges, however, present obstacles to achieving these capabilities. The first challenge is that mobile devices offer less computational power than a conventional desktop or server computer. A second challenge is that computation-intensive tasks, such as image recognition or even global positioning system (GPS), take a heavy toll on battery power. The third challenge is dealing with unreliable networks and bandwidth. This post explores our research to overcome these challenges by using cloudlets, which are localized, lightweight servers running one or more virtual machines (VMs) on which soldiers can offload expensive computations from their handheld mobile devices, thereby providing greater processing capacity and helping conserve battery power.

This leverage of external resources to augment the capabilities of resource-limited mobile devices is a technique commonly known as cyber-foraging. The use of VM technology provides greater flexibility in the type and platform of applications and also reduces setup and administration time, which is critical for systems at the tactical edge. The term tactical edge refers to systems used by soldiers or first responders that are close to a mission or emergency executing in environments characterized by limited resources in terms of computation, power and network bandwidth, as well as changes in the status of the mission or emergency.

Cloudlets are located within proximity of handheld devices that use them, thereby decreasing latency by using a single-hop network and potentially lowering battery consumption by using WiFi instead of broadband wireless which consumes more energy. For example, a cloudlet might run in a Tactical Operations Center (TOC) or a Humvee. From a security perspective, cloudlets can use WiFi networks to take advantage of existing security policies, including access from only specific handheld devices and encryption techniques.

Related work on offloading computation to conserve battery power in mobile devices relies on the conventional Internet or environments that tightly couple applications running on handheld devices and servers on which computations are offloaded. In contrast, cloudlets decouple mobile applications from the servers. Each mobile app has a client portion and an application overlay corresponding to the computation-intensive code invoked by the client. On execution, the overlay is sent to the cloudlet and applied to one of the virtual machines running in the cloudlet, which is called dynamic VM synthesis. The application overlay is pre-generated by calculating the difference between a base VM and the base VM with the computation-intensive code installed. The only coupling that exists between the mobile app and the cloudlet is that the same version of the VM software on which the overlay was created must be used. Since no application-specific software is installed on the server, there is no need to synchronize release cycles between the client and server portions of apps, which simplifies the deployment and configuration management of apps in the field.

Dynamic VM synthesis is particularly useful in tactical environments characterized by unreliable networks and bandwidth, unplanned loss of cyber foraging platforms, and a need for rapid deployment. For example, imagine a scenario where a soldier needs to execute a computation-intensive app configured to work with cloudlets. At runtime, the app discovers a nearby cloudlet located on a Humvee and offloads the computation-intensive portion of code to it. Due to enemy attacks, network connectivity, or exhaustion of energy sources on the cloudlet, however, the mobile app is disconnected from the cloudlet. The mobile app can then locate a different cloudlet (e.g., in a TOC) and—due to dynamic VM synthesis—can have the app running in a short amount of time, with no need for any configuration on the app or the cloudlet. This flexibility enables the use of whatever resources become opportunistically available, as well as replacement of lost cyber-foraging resources and dynamic customization of newly-acquired cyber foraging resources.

As part of our research, we are focusing on face recognition applications. Thus far we have created an Android-based facial recognition app that performs the following actions:

1. It locates a cloudlet via a discovery protocol
2. It sends the application overlay to the cloudlet where dynamic VM synthesis is performed.
3. It captures images and sends them to the facial recognition server code that now resides in the cloudlet.
4. The application overlay is a facial recognition server written in C++ that processes images from a client for training or recognition purposes. When in recognition mode, it returns coordinates for the faces it recognizes, as well as a measure of confidence. The first version of the cloudlet is a simple HTTP server that receives the application overlay from the client, decrypts the overlay, decompresses the overlay, and performs VM synthesis to dynamically set up the cloudlet.

The first phase of our work has focused on creating the cloudlet prototype described above. In the second phase we will conduct measurements to see if computations in a cloudlet provide significant reductions in device battery power. In addition, we will gather measurements related to bandwidth consumption of overlay transfer and VM synthesis to focus on optimization of cloudlet setup time. Assuming we are successful, our third phase will create a cloudlet in the RTSS Concept Lab to explore other ways to take computation to the tactical edge.

As part of our research, we are collaborating with Mahadev Satyanarayanan, the creator of the cloudlet concept and a faculty member at Carnegie Mellon University's School of Computer Science. We will be blogging about the progress of our research in future posts.

Additional Resources:

To read more about the cloud computing research conducted by the SEI's System of Systems team, please visit www.sei.cmu.edu/sos/research/cloudcomputing/

To view an SEI Webinar on cloud computing, please visit www.sei.cmu.edu/library/abstracts/webinars/Cloud-Computing.cfm

Related Web Sites

http://blog.sei.cmu.edu/archives.cfm/category/cloud-computing

For General Information

For information about the SEI and its products and services, contact
Customer Relations
Phone: 412-268-5800
FAX: 412-268-6257
customer-relations@sei.cmu.edu
www.sei.cmu.edu

07/28/2011

Regression Verification of Real-time Embedded Software

By Arie Gurfinkel, Senior Member of the Technical Staff, Research Technology and System Solutions (RTSS)

Continuous technological improvement is the hallmark of the hardware industry. In an ideal world—one without budgets or schedules—software would be redesigned and redeveloped from scratch to leverage each such improvement. But applying this process for software is often infeasible—if not impossible—due to economic constraints and competition. This posting discusses our research in applying verification, namely regression verification, to help the migration of real-time embedded systems from single-core to multi-core platforms.

A key recent technological hardware improvement is the advent of larger multi-core architectures. In theory, software written for single-core hardware should be reused as-is on multi-core hardware. After all, software that has been validated extensively on single-core hardware—and is not being modified—should behave unchanged on multi-core hardware. In practice, however, this migration isn't so easy due to many factors that influence software behavior, including the architectural assumptions made by the underlying hardware. Multi-threaded programs are particularly problematic since key assumptions (such as one-at-a-time thread execution) made when these programs were developed for a single core are often invalidated by the true parallelism of multi-core hardware.

Reusing software written for single-core hardware can be dangerous without first verifying that it works correctly on multi-core hardware. At the SEI we've seen many instances where software ported from single- to multi-core hardware is less robust than its single-core counterpart. Addressing this problem is increasingly essential for the Department of Defense (DoD). The DoD is one of the largest users of software—especially mission- and safety-critical real-time embedded software where the consequences of defects can be deadly and the right answer delivered too late becomes the wrong answer.

Formal verification techniques ensure that a program will work. These techniques use mathematical models of programs to prove (or disprove) that the software will function correctly under certain conditions. Although verification provides strong guarantees of correctness, the verification process itself is expensive and time-consuming, in part due to a lack of scalable automated tools and the need for formal specifications.

Over the next year, my colleagues and I plan to study an application of a particular formal verification technique known as regression verification by applying it to the problem of migrating real-time embedded software from single- to multi-core hardware. Regression verification involves deciding the behavioral equivalence of two, closely related programs, e.g., Pold and Pnew. This technique is potentially simpler in practice than applying functional verification to Pnew against a user-defined, high-level specification since it circumvents the complex and error-prone problem of creating specifications. Moreover, this technique is also potentially more scalable since the computational effort will ideally be proportional to the difference between Pnew and Pold, rather than the size of Pold, as is the case with conventional testing and functional verification techniques.

Joining me on this project will be Sagar Chaki and Dionisio de Niz, senior members of the technical staff in the SEI Research, Technology, and System Solutions (RTSS) program, together with Ofer Strichman, a visiting scientist in RTSS and the co-inventor of regression verification. Based on our work thus far, regression verification appears particularly relevant when migrating from single-core to multi-core hardware in safety-critical domains, such as real-time embedded systems, where validation is necessary (and costly using conventional verification techniques). Moreover, real-time embedded systems are often highly restricted (e.g., they use limited programmatic features and specific task scheduling disciplines) and these restrictions can be leveraged to improve the tractability of regression verification.

Our goal over the next year is to explore the application of regression verification to software migration across hardware platforms. We will work with Professor Strichman to develop regression verification algorithms for multi-core hardware migration. We will also develop and test a formal definition of regression verification for migration of real-time embedded systems from single-core to multi-core hardware.

Addressing the single-core to multi-core migration problem is crucial for DoD and industry. One of the biggest challenges that both face is migrating complex cyber software infrastructure to leverage the latest hardware capabilities, such as multi-core. I will blog about the progress of our research throughout the course of the year.

Related Web Sites

http://blog.sei.cmu.edu/post.cfm/regression-verification-of-real-time-embedded-software

For General Information

For information about the SEI and its products and services, contact
Customer Relations
Phone: 412-268-5800
FAX: 412-268-6257
customer-relations@sei.cmu.edu
www.sei.cmu.edu

08/15/2011

T-Check: Low-Cost Approach to Technology Evaluation

Do you know whether the technology you plan to use will work in your context?

Do you want to verify claims made about technologies?

Do you think that it will be too costly or take too long to investigate technologies you want to use?

Today, most organizations are looking to become more agile and "do more with less" in order to stay competitive. As they look ahead, leading organizations rely on a proven approach to improved productivity and reduced cost—using the latest technology.

So, if your organization depends more and more on new or emerging technology, you'll want to know how you can be assured about the claims made for it. Will the technology work as promised and as expected in your organization's context? Will it allow you to easily modify your business processes, for example… or leverage your existing investments… or deliver platform independence?

T-Check: A Way to Test Technologies

The Carnegie Mellon® Software Engineering Institute (SEI) offers T-Check℠ investigations as an effective way to evaluate the appropriateness of a technology in your context.

T-Check investigations are experiments situated in a specific context, with the goal of providing a sanity check on a technology's claims.

T-Check experiments are ruthlessly efficient; they are simple investigations that provide insight into technologies without requiring a large investment.

The T-Check approach is like the classic scientific method in that it involves (as shown in Figure 1)

1. formulating hypotheses about the technology
2. examining these hypotheses against very specific criteria through experimentation
3. drawing conclusions from the test data about the usefulness of a technology in a certain context

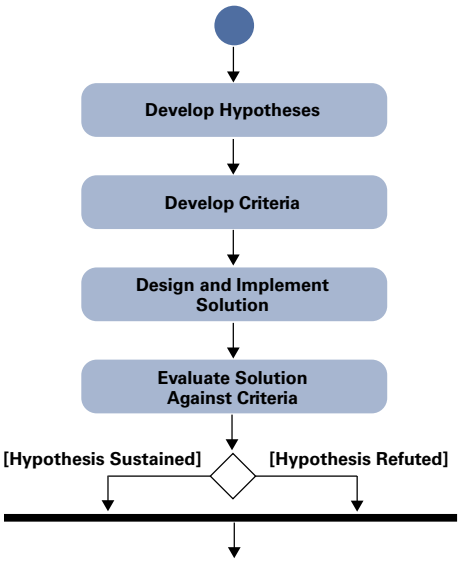


Figure 1: The T-Check Approach

You should consider the T-Check approach especially if you are planning for system-of-systems interoperability—through, for instance, an SOA infrastructure acquisition or a migration to an SOA environment, where many of the technologies and standards supporting SOA are still considered emergent.

Two Example T-Check Investigations

The System of Systems Engineering (SoSE) team at the SEI has performed T-Check experiments on some popular technologies for systems interoperability, including the following: Model-Driven Architecture and Web Services.

Model-Driven Architecture

For the specified conditions and through the T-Check approach, the hypothesis that the use of MDA reduces development time was partially refuted. Development time can increase greatly for the first application on which MDA is used, due to configuration and transformation modifications. The approach also refuted the hypothesis that the use of MDA frees the developer from understanding low-level details of the target platform and underlying infrastructure.

Web Services

For the conditions tested, the evaluation team determined that Web Services technology is fairly easy to implement. Likewise, it is simple to connect applications developed on different platforms using Web Services. The relative ease of implementing and using this technology is possible because Web Services elements are based on widely accepted standards that are supported by a large number of vendors. Nonetheless, the standards behind Web Services are still maturing. The T-Check approach also showed that too few public Web Services are available, and most of those available are poorly documented and of poor quality. (For more on this T-Check investigation, see the reverse side.)

Benefits of the T-Check Approach

- **The simplicity of experiments allows early insight into technologies without a huge investment.**
- **Clear hypotheses and criteria avoid time wasted "playing" with technologies.**
- **The additional findings are often greater than the direct results of the experiments.**
- **People conducting the experiments acquire early competence with the technology.**

T-Check: Low-Cost Approach to Technology Evaluation

T-Check Investigation of Web Services

Context for the Investigation: a military human resources system

Table 1: Hypotheses and Criteria

Hypothesis	Criteria
It is fairly easy for developers to connect applications developed for the same platform using Web Services.	• Documentation is available on how to implement and access Web Services in the selected platform. • Tools and libraries are available to implement Web Services in the selected platform. • Tools and libraries are available to generate code in the selected platform to access a Web-based service from the associated WSDL document that describes the service. • Two applications can connect using Web Services.
There are several public, easily discoverable, and high-quality Web Services that can be used in applications. (High-quality Web Services are those for which the interfaces are well documented and straightforward to use.)	• Developers are able to locate Web Services for use in their application by using public UDDI repositories or searching on the Internet. • The Web Services are well documented, and there is guidance on how to use them.
There are no problems relating to data types if Web Services are used to connect applications on different platforms (e.g., J2EE and .NET)	• The two applications can exchange complex, date, and floating point data types with no data inconsistencies between the two platforms. • The exchange can be done using default mechanisms provided with the Web Services tools and libraries.

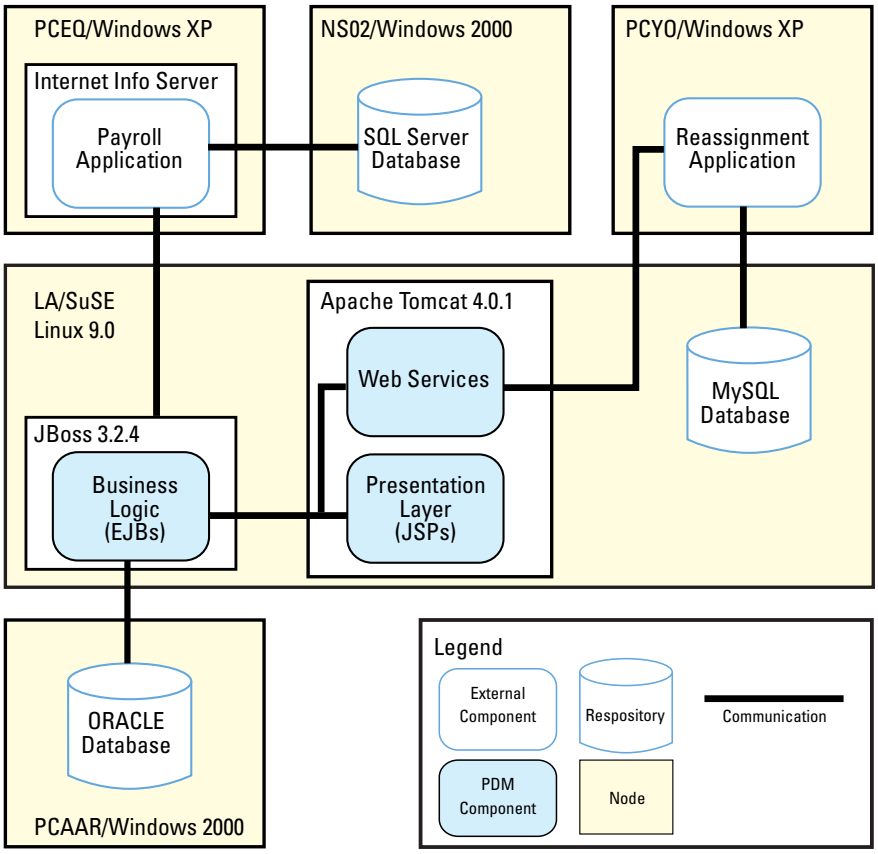


Figure 2: Deployment View of Model Solutions for T-Check Investigation of Web Services

Related Website

www.sei.cmu.edu/interoperability/casestudies/techeval/

For General information

For general information about the SEI and its products and services, contact

Customer Relations
P: 412–268–5800
F: 412–268–5758
www.sei.cmu.edu
Software Engineering Institute
4500 Fifth Avenue
Pittsburgh, PA 15213-2612

T-Check Reports

Model Problems in Technologies for Interoperability: Web Services (CMU/SEI-2006-TN-021).
http://www.sei.cmu.edu/library/abstracts/reports/06tn021.cfm

Model Problems in Technologies for Interoperability: OWL Web Ontology Language for Services (OWL-S) (CMU/SEI-2006-TN-018).
http://www.sei.cmu.edu/library/abstracts/reports/06tn018.cfm

Model Problems in Technologies for Interoperability: Model-Driven Architecture (CMU/SEI-2005-TN-022).
http://www.sei.cmu.edu/library/abstracts/reports/05tn022.cfm

T-Check in Technologies for Interoperability: Business Process Management in a Web Services Context (CMU/SEI-2008-TN-005).
http://www.sei.cmu.edu/library/abstracts/reports/08tn005.cfm

T-Check in Technologies for Interoperability: Web Services and Security—Single Sign-On (CMU/SEI-2008-TN-026).
http://www.sei.cmu.edu/library/abstracts/reports/08tn026.cfm

T-Check for Technologies for Interoperability: Open Grid Services Architecture (OGSA)—Part 1 (CMU/SEI-2007-TN-016).
http://www.sei.cmu.edu/library/abstracts/reports/07tn016.cfm

A Process for Context-Based Technology Evaluation (CMU/SEI-2005-TN-025).
http://www.sei.cmu.edu/library/abstracts/reports/05tn025.cfm

System of Systems (SoS) Architecture Definition and Evaluation

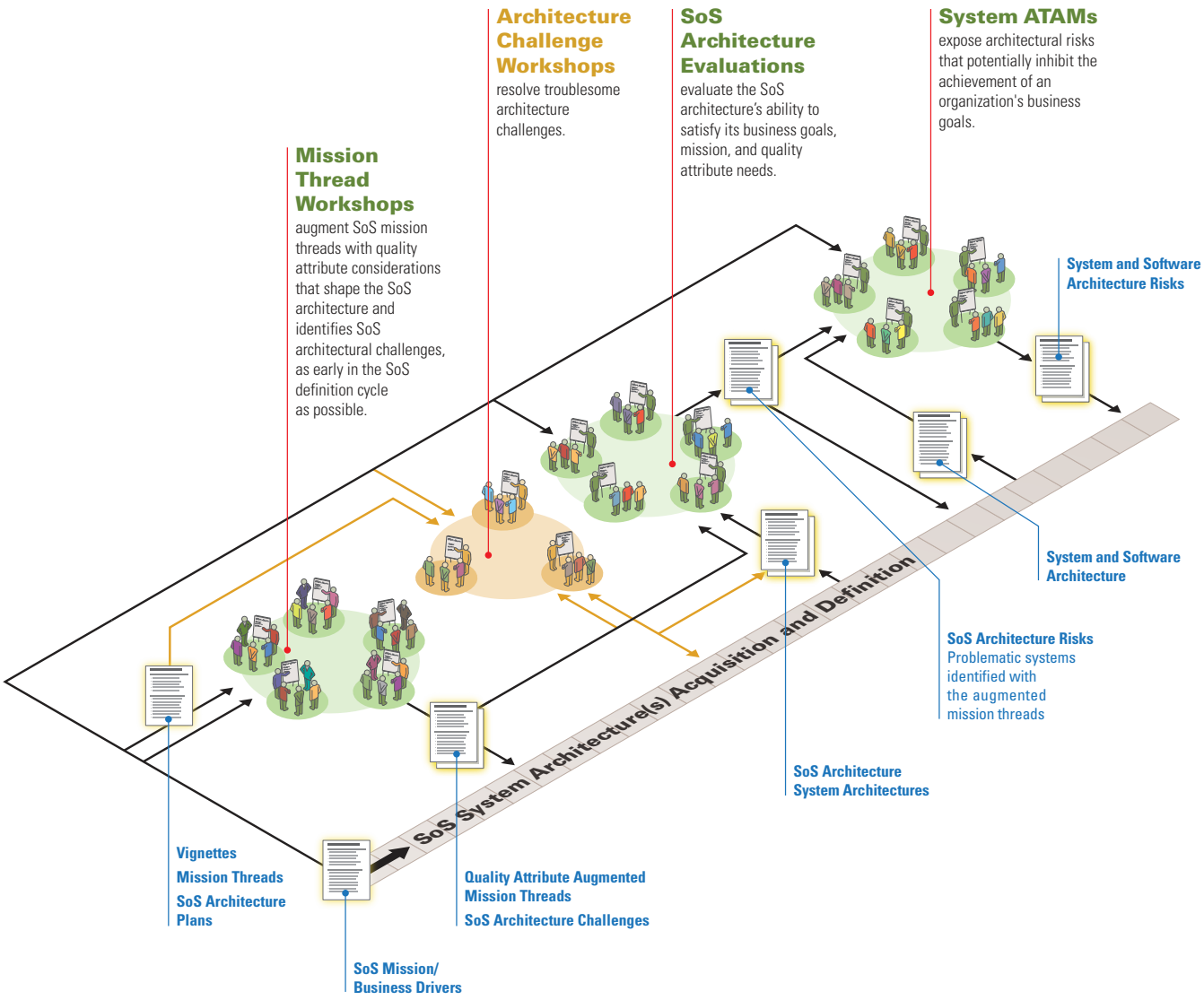
Have you ever encountered symptoms such as these?

- Communication bottlenecks under various load conditions that dramatically increase access time to critical capabilities
- Systems that hang up or crash causing warfighters to be without situational awareness during overly long recovery times
- Persistently unpredictable and unpleasant side-effects in portions of the SoS that distract warfighters from their primary focus
- Trouble sticking to an integration schedule during development
- Difficulty identifying the root causes of integration problems, resulting in the proliferation of patches and workarounds during integration and test

These common symptoms are indications of architectural deficiencies in systems of systems. If you have experienced these symptoms before, or if you want to identify the technical risks in your system of systems and avoid them in the future, the SEI can help.

Quality Attributes: the key to mission success

In addition to providing needed capabilities, all systems, including systems of systems (SoS), must satisfy non-functional quality attributes that are essential to mission success and achievement of business goals. Examples of such quality attributes are performance, availability, reliability, security, usability, testability, safety, interoperability, maintainability, and spectrum management.



System of Systems (SoS) Architecture Definition and Evaluation

Severe integration, interoperability, and operational problems can arise from inconsistencies, ambiguities, and omissions in addressing the quality attributes of SoS architectures. In many cases, the root causes of interoperability and integration problems in systems of systems can be traced to a failure to address quality attributes in the architectures.

DoDAF and system use cases aren't enough

DoDAF and system use cases are common architecture/design practices that are used to identify and develop needed SoS capabilities. However, these practices do not adequately address cross-cutting quality attributes in an SoS. To be sure that systems will satisfy both their functional and non-functional requirements, developers need to consider quality attributes in the context of end-to-end mission threads.

SEI Engagement: SoS Architecture Definition and Evaluation

The SEI is currently piloting a multi-phased engagement process that can be applied throughout the stages of the architecture-definition life cycle. In its early phases, this engagement includes Mission Thread Workshops, Architecture Challenge Workshops, SoS Architecture Evaluations, and System ATAMs.

The purpose of a Mission Thread Workshop (MTW) is to augment end-to-end missions threads with quality attribute considerations and identify architecture, engineering, and capability challenges early in the definition of a system of systems architecture. An MTW brings together key stakeholders representing a variety of organizations, roles, and points of view. Together, these stakeholders augment end-to-end mission threads by considering and capturing quality attribute, mission, and capability needs. The information elicited in an MTW is then made available to the SoS architecture development, integration, and test activities. The information is also reduced to a set of five to seven architectural challenges to inform system and software architecture development and acquisition.

The architectural challenges developed in the MTW will have undergone a review and been subdivided in terms of (at least) importance, difficulty, and timeliness. The Architecture Challenge Workshop (ACW) takes one or more of these challenges, either together or sequentially, and engages a small team of stakeholders in collectively organizing an approach to resolving the challenges. Challenges are turned into technical action items and assigned to working groups, with a schedule and a review process to ensure closure of the challenges and introduction of technology to overcome them.

The purpose of the SoS Architecture Evaluation is to evaluate the SoS architecture's ability to satisfy its business goals, mission, and quality attribute needs. It identifies architectural risks, using the augmented mission threads and architectural challenges developed in previous MTWs. The evaluation provides early identification of SoS architecture risks and identifies problematic systems and SoS components. The architects, along with the program office, can then identify, prioritize, and mitigate risks early in the life cycle, before integration. Working early with the program office to develop a sound architecture-centric acquisition strategy and associated artifacts motivates contractors to do the right thing architecturally. It also gives the program office visibility into the progress of SoS architecture definition.

In most cases, an SoS will include many legacy systems whose management is separate from the SoS management and that were developed with a different set of quality attribute requirements from the usage envisioned within the SoS. Some of these legacy systems may be used as is, while others may require some changes (either to the legacy system or the SoS) in order to work coherently within the SoS. Architectural risks for legacy systems within an SoS can be identified early in the SoS life cycle by conducting System ATAMs on critical legacy systems. The System ATAMs use the quality-attribute-augmented SoS mission threads developed in the MTW as a basis for scenarios in the architecture evaluation.

In addition to these early-phase activities, the SEI's support for SoS development and evaluation includes attention to architecture and quality attributes throughout a program's life cycle. The SEI's approach is flexible and tailorable, and has been proven effective on a number of DoD SoSs (e.g., Navy CG(X), Army PM Battle Command, and Lockheed Martin).

Contact the SEI now

For more information about how you can engage with the SEI to reduce your technical risk and support development of your system of systems, contact

Software Engineering Institute
Carnegie Mellon University
4500 Fifth Avenue
Pittsburgh, PA 15213-2612
P: 412-268-5800
F: 412-268-5758
W: www.sei.cmu.edu
E: customer-relations@sei.cmu.edu

Software Engineering Institute | Carnegie Mellon

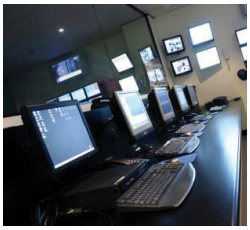
More Accurate Prediction of Security

Through Architecture Analysis using Model-Based Engineering Tools

Security Challenges

A system designer faces several challenges when specifying security for distributed computing environments or migrating systems to a new execution platform.

Business stakeholders impose constraints due to cost, time-to-market requirements, productivity impact, customer satisfaction concerns, and the like. And users exercise power at the desktop over computing resources and data availability.



So, a system designer needs to understand requirements regarding protected resources (e.g., data), confidentiality, and integrity.
And, a designer needs to predict the effect that security measures will have on other runtime quality attributes such as resource consumption, availability, and real-time performance.

After all, the resource costs associated with security can easily overload a system. Security processing can increase usage of processing power, bandwidth, battery (in embedded systems), and other resources.

Despite that, security is often studied only in isolation and late in the process. However, the SEI has developed model-based engineering (MBE) tools, methods, and analytical techniques to validate security according to flow-based approaches and standard security protocols such as Bell-LaPadula, Chinese Wall, and role-based access control.

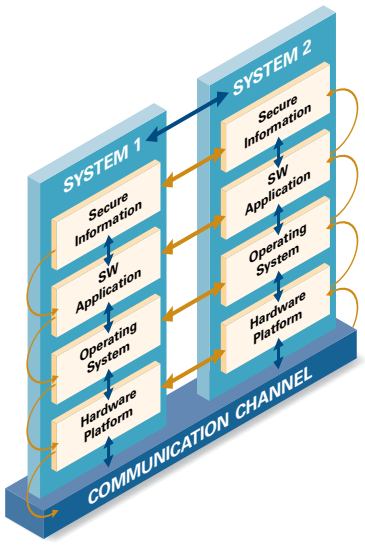
The SEI uses model-based engineering tools, methods, and techniques to more accurately predict system security.

Security Prediction with Less Cost, Less Risk, Increased Confidence

Security analysis using SEI MBE tools, methods, and techniques allows software validation by identifying data elements to be protected, components that should be allowed access to those elements, and appropriate communication channels.

This analysis permits the designer to enforce security at the minimum level required, use sanitization, and map software architecture to hardware.

MBE also allows a designer to identify how security choices affect other quality attributes. For example, a designer can visualize and analyze, for battery-powered devices in embedded systems, the tradeoff between increased execution time and latency that supports the required security levels—to take advantage, for instance, of the multiple independent levels of security (MILS) paradigm.



Security Analysis Concern	SEI MBE	Answer
Sanitization (i.e., controlled lowering of security levels)	✔	Provides metrics on the number of sanitized flows in a system
Security effectiveness applied using minimum security clearances	✔	Derives the minimum security clearance on components in the model (By pointing out differences between actual security clearances and the minimum security clearance required, a system designer can evaluate security effectiveness.)
Integration of security at multiple system levels	✔	Provides system-level solution by checking that secure information is associated with components that have appropriate security clearance and is communicated by secure connections

Read more
Building Secure Systems using Model-Based Engineering and Architectural Models at http://www.stsc.hill.af.mil/crosstalk/2008/09/0809HanssonFeilerMorley.html

Modeling System Architectures Using the Architecture Analysis and Design Language (AADL)
For Course Registration
www.sei.cmu.edu/training/p72.cfm

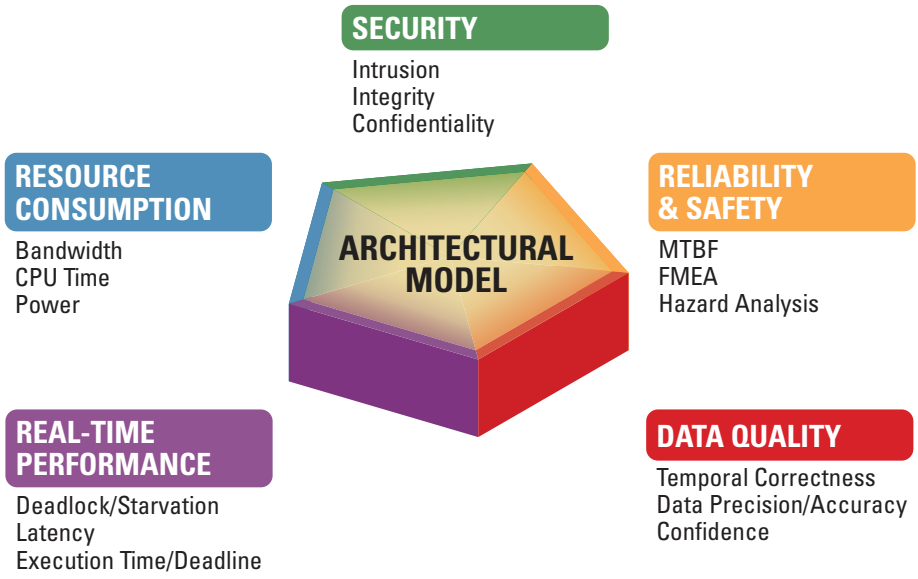
This course may also be offered by arrangement at customer sites. Email course-info@sei.cmu.edu or call +1 412-268-7622 for details.

For More Information
Customer Relations
Phone: +1 412-268-5800
FAX: +1 412-268-6257
customer-relations@sei.cmu.edu

Software Engineering Institute
4500 Fifth Avenue
Pittsburgh, PA 15313-2612
www.sei.cmu.edu

More Accurate Prediction of Security

Through Architecture Analysis using Model-Based Engineering Tools



The SEI MBE Toolkit

The SEI uses the ***Architecture Analysis & Design Language (AADL)*** to document a system architecture and provide a platform for multiple analyses.

The AADL, an international industry standard, supports multiple analyses from a single architectural model, enables modeling and analysis throughout the life cycle, and provides analysis of runtime behavior (what) rather than functional behavior (how).

Through its ***XML/XMI interchange format,*** the AADL supports model interchange and tool chaining. And, the SEI offers the freely available ***Open Source AADL Tool Environment (OSATE)*** set of analysis plug-ins. The OSATE security analysis plug-in checks the security levels and flow completeness of components.

The SEI has developed OSATE as a set of plug-ins for processing AADL models that includes:

- a syntax-sentitive text editor, with integrated error reporting
- a parser and semantic checker for textual AADL with conversion into AADL XML
- an unparser for AADL XML to textual AADL conversion
- support for multi-enterprise development through a version control system interface

The AADL also can be used with

- UML state and process charts through its UML profile
- the SEI Architecture Tradeoff Analysis Method®, to drill into root causes and develop quantitative analysis
- assurance cases, to support claims made about the safety, security, or reliability of a system

Prevent System Integration Problems and Simplify Life-Cycle Support

Modeling of system quality attributes is often done—when it is done—with low-fidelity software models and disjointed architectural specifications by various engineers using their own specialized notations.

These models are typically not maintained or documented throughout the life cycle, making it difficult to predict the impact of change on attributes that cut across system functionality. The unanticipated effects of design approaches or changes are discovered only late in the life cycle, when they are much more expensive to resolve.

Analysis of a *system architecture model* offers a better way to predict the behavior of quality attributes. The SEI approach to model-based engineering (MBE) allows analysis

- using a single architecture model
- early and often in the development life cycle or on an existing system architecture
- at different architecture refinement levels
- along diverse architectural aspects such as behavior and throughput

Integration is a major cost and risk in complex systems. System understanding is a major cost driver during system maintenance. Proper use of MBE tools can prevent system integration problems and simplify life-cycle support.

System Architecture Modeling and Analysis

The Carnegie Mellon® Software Engineering Institute (SEI) provides technical assistance and guidance to transform the architectural design process from one based on human evaluation to one based on automated analysis.1

This analysis includes

- validating system quality attributes early in the design phase
- facilitating system integration
- conducting impact and tradeoff analysis using architecture models

For predicting and validating specific nonfunctional properties using model-based engineering, the SEI can help you to

- perform analysis that gives greater assurance that deployment will succeed
- evaluate fault tolerance of architectures
- adopt analytical resource models to validate performance behavior, power consumption, and network bandwidth usage
- model security aspects of architecture
- conduct analysis to guide localized architectural change
- validate data quality requirements such as temporal correctness, accuracy/precision, and confidence

Put MBE to work on your projects quickly!
Register for training by the Software Engineering Institute.
Go to www.sei.cmu.edu/training/p72.cfm.

1 One large defense contractor, for instance, blames human interpretation of the complexity involved with embedded systems for decreasing productivity to 6 or fewer lines of code per day.

0003-2010-03

For more information:
Software Engineering Institute
Carnegie Mellon University
4500 Fifth Avenue
Pittsburgh, PA 15213
412.268.5800
info@sei.cmu.edu
www.sei.cmu.edu