The Interplay of Architecture, Security, and Systems Engineering

Rick Dove, theme editor, rick.dove@incose.org
Cochair, System Security Engineering Working Group

Today, all systems are prey. It matters not their intended purpose and function. Technology is their Achilles heel. Technology is their vector of downfall. They are defenseless in an age of guerrilla warfare, technologically empowered individuals, rapid technology development, do-it-yourself affordability, readily accessible knowledge, global infrastructure networks, and the human hacker inclination to re-purpose a system just because it's there.

Systems engineering is awesome. We stand in wonder at the good we can build. In time we find that this respect and awe is not shared by all. Some take equal fulfillment in destruction or exploitation, no matter the motivation. The modern response is after-the-breech correction and watchdog shepherding. Even the weapon-bristling naval system is humbled by the rubber-rafted bomb.

In days of old the important systems embedded security in the architecture: fortress cities, castles, booby-trapped tombs. Security had high priority in the system engineering trade-space. Security was rooted in fundamental requirements and values. The technologies of construction and destruction were on a level playing field. With the scientific age the development of technology by those who practiced construction outpaced the efforts of those who focused on destruction. The entry barriers of resource and knowledge favored socially-developed countries and high-visibility activities. Embedded system security was unnecessary, and atrophied as a practice. Now we have come full circle, as technically literate and adept practitioners have again leveled the playing field of construction and destruction, of protection and exploitation.

It is past time that system engineering reclaim and embrace the responsibility for system security. Technology advancement discovers new vulnerability and exploitation faster than systems can respond. Flatfooted, they sit as prey. Stone and mortar castle architecture would not suffice today, nor city fortress emplacement architecture.

These essays are intended to open the door on architecture as the first enabler or impeder of system security. No amount of subsystem engineering and reengineering or external protection can overcome a security-ignorant system architecture. There are other areas of system engineering that need security attention, but the impact of architecture makes it an appropriate start. The intent of this theme section is to begin the process of reintegrating security engineering into the system engineering trade space, and to bring security engineering out of the shadows.

Security in the Headlines

All of us can easily relate system security issues to identity theft, bank account leakage, personal computer infections, and invaded enterprise networks. Many of us deal daily with the physical security of identity badges and restricted entry ways, document classifications and information leakage, metal detectors, forbidden personal electronics, and interactions with security guards. Some of us have been sensitized to the extreme in jobs where defense and government compromise would have intolerable societal effect. But none of us have found a safe haven.

A thirty-day slice of recent news demonstrates the growing breadth of the security problem for today's systems:

- 8 April 2009, *Wall Street Journal*: "Cyberspies have penetrated the U.S. electrical grid and left behind software programs that could be used to disrupt the system, according to current and former national-security officials" (Siobhan Gorman, http://online.wsj.com/article/SB123914805204099085.html).

- 9 April, *San Jose Mercury News*: "Somebody opened a manhole in South San Jose, climbed down eight to 10 feet and cut four or five fiber-optic cables. Britton [of the San Jose Police Department] also said there was a report of underground cables being cut in San Carlos. The outage initially affected some cell phones, Internet access and about 52,200 Verizon household land lines in Morgan Hill, Gilroy and Santa Cruz County. ATMs in South Santa Clara County were not working. Saint Louise Regional Hospital in Gilroy cancelled all elective surgeries in response to the emergency, according to county officials" (M. Gomez, K. McLaughlin, and J. P. Sulek, www.mercurynews.com/localnewsheadlines/ci_12106300).
- 20 April, *Wired*: "Brazilian satellite hackers use high-performance antennas and homebrew gear to turn U.S. Navy satellites into their personal CB radios."—and have been doing it for years on a large cultural scale (Marcelo Soares, www.wired.com/politics/security/news/2009/04/fleetcom).
- 21 April, *Wall Street Journal*: "Computer spies have broken into the Pentagon's $300 billion Joint Strike Fighter project -- the Defense Department's costliest weapons program ever… Similar incidents have also breached the Air Force's air-traffic-control system in recent months." (S. Gorman, A. Cole, and Y. Dreazen, http://online.wsj.com/article/SB124027491029837401.html).
- 23 April, *CNET News*: "The Conficker worm infected several hundred machines and critical medical equipment in an undisclosed number of U.S. hospitals recently… It is unclear how the devices, which control things like heart monitors and MRI machines…got infected." A case of unintended collateral damage (Elinor Mills, http://news.cnet.com/8301-1009_3-10226448-83.html).
- 23 April, *Popular Science*: "For years, the U.S. intelligence community worried that China's government was attacking our cyber-infrastructure. Now one man has discovered it's worse: It's hundreds of thousands of everyday civilians. And they've only just begun" (Mara Hvistendahl, www.popsci.com/scitech/article/2009-04/hackers-china-syndrome).
- 30 April, National Public Radio: "Piracy financiers are usually ethnic Somali businessmen who live outside the country and who typically call a relative in Somalia and suggest they launch a piracy business. The investor will offer $250,000 or more in seed money, while the relative goes shopping… for arms, boats, employees, intelligence, and professional negotiators" (Chana Joffe-Walt, www.npr.org/templates/story/story.php?storyId=103657301).
- 7 May, *CNET News*: "Hackers have broken into the air traffic control mission-support systems of the U.S. Federal Aviation Administration several times in recent years, according to an Inspector General report sent to the FAA this week." Just because they could? Or probing for later? (Elinor Mills, http://news.cnet.com/8301-1009_3-10236028-83.html).

The Somalia pirate story may have seemed out of place if you were inclined to associate security attacks with computer systems. But today's security battle is over the *control* of systems, of all kinds: those in our planes, trains and automobiles; in power generation equipment and in manufacturing systems; in every facet of communications from telephone to television, from satellite to Internet; in our transportation infrastructure from ocean shipping to package delivery and traffic signals; and of course the machines of war that defend us when operational and pointed in the right direction.

We can't blame the security engineering community for falling behind—they've been knocking on the system engineering door for a long time. It's time to let them in.

A Taste of New Thinking

System Security Engineering: A Critical Discipline of Systems Engineering

Kristen Baldwin opens with a revealing perspective on the changing nature of systems. Kristen serves as Deputy Director for Strategic Initiatives in the office of the U.S. Deputy Under Secretary of Defense for Acquisition and Technology, Systems and Software Engineering Directorate. Technology advancement is relentless, as she observes: "Twenty years ago, systems were relatively stand-alone, software was critical but not prevailing, and the supply base was known and traceable. Prime contractors build today's complex, software-controlled, highly networked systems by integrating hundreds of suppliers and commercial-off-the-shelf (COTS) components, whose origin and level of integrity are difficult to ascertain. Security vulnerabilities now exist beyond the mitigations that information assurance controls typically provide. They present themselves in embedded software and hardware components and in system-of-systems architecture designs." Kristen brings us up to speed on initiatives in process, and closes with an urgent call to arms: "This information-age threat challenges the engineering community to treat security as a consideration in the risk and design trade space… As threats evolve, so must our advancements in the field of system security engineering."

Embedding Agile Security in System Architecture

A rising call is being heard for a new generation of integrated system security embedded in… what? In architecture? What does that mean—modern day castles? In my own contribution to this theme section I depict a generic architecture for any system that would be agile, and suggest five defining characteristics for embedded agile security: self-organizing, adaptable to threat variations, evolvable in pace with possibility, proactive as well as reactive, and in harmony with system purpose. This agile-system architecture is shown as sustained by four active functions. These functions are suggested as proper seats for embedding security. 20 years of independent study and practice in agile system architecture are behind these suggestion, and form the basis for two graduate courses at Stevens Institute of Technology while independent study and practice continue.

Toward a Dynamic System Architecture for Enhanced Security

During World War II, Germany employed a field radio design that was functionally perfect, with sheathed-wire pairs, lever-driven closure cams, and engineering excellence for crystal-clear communications. By contrast, the U.S. radio designers skimped, using a single bare iron wire strung between radios, with the earth as the return ground. This U.S. setup produced weak, static-laced sounds that were easily overwhelmed by the roar of battle. On the other hand, any U.S. grunt could quickly twist the broken pieces of an iron wire together to restore severed communication, while the interdiction of the German high-performance communication channel was a difficult breech for them to overcome. Other engaging stories illustrate Mark De Spain's point that systems live in a world that will have its way with them, and design must expect the need to adapt, even without a clear definition of what reality may bring. Mark's work at Sandia National Labs is about sustainable system service, under uncertain conditions. He is also current president of the Albuquerque INCOSE chapter and is pursuing a doctorate in systems engineering at Stevens Institute of Technology.

Resilient Control Systems: A Basis for Next-Generation Secure Architectures

Control systems are generally focused on driving a system along a desired path of performance. Sensors measure the performance state, and feedback loops adjust accordingly. Craig Rieger, from Idaho National Labs, suggests that this practice is myopic, and calls for a system to have a much broader sense of awareness. Resilience in the face of intelligent, targeted interdiction as well as in response to the fallibility of reactions and interpretations is his objective. Following lines of thought developed in

workshops at the 2008 First International Conference on Resilient Control Systems, Craig recognizes that designs traditionally focused on failure risks due to accidents now need to focus on risks from attack.

Secure Architecture and Design of Component-Based Systems

Hardware and software component-based architectures offer alluring advantages, but also bring the potential for new types of vulnerabilities and risks from component interactions and emergent behaviors. Whether built to order by trusted groups or acquired in COTS fashion, components that pass security tests individually may still contribute to emergent vulnerabilities and risks when combined with others. Certified as an Information Systems Security Professional (CISSP), Karen Goertzel thinks about these things at Booz Allen Hamilton, but uses a systems engineer's total-system point of view.

Using DoDAF to Build Security into the Lifecycle

Systems are expected to deliver services, but too often the focus is on delivering validated conformance to requirements—at the time of delivery acceptance. "The security of a system, perhaps more than other functional and performance requirements, challenges the systems engineer to consider the operational phase of a system's lifecycle." So says Bill Mulokey, who brings a forty-year experience base with certifications in both enterprise architecture (CEA from the Federated Enterprise Architecture Institute) and information systems security (CISSP from International Information Systems Security Certification Consortium). He was Booz Allen Hamilton's participant in a recent NextGen Air Traffic Management weather-based requirements study that was integrated with the U.S. Department of Defense Architecture Framework. Notably, here Bill deals with system designs that must evolve throughout their lifecycles, and shows how security adaptation is enabled and facilitated by system architecture.

An Architecture of Information Assurance Processes

Processes are systems, and they are better systems when principles and best practices are employed to craft their architecture. In a contribution funded by his employer, Mitre, Jackson Wynn organizes the many U.S. Department of Defense information assurance processes for acquisition into a layered architecture, showing current overlaps and proposing a rationalization. Importantly, he calls "for security awareness training to start earlier in the system-development lifecycle, with training geared toward those engineering personnel who design and implement DoD information systems." As a lead information security engineer at Mitre, Jackson developed an agile security-policy enforcement prototype; a promising fit with the System Security Engineering Working Group's emphasis on next-generation agile security. Jackson played an active role in reviewing the symposium presentations made by the essay authors at IW09.

Standardized Practices for Embedding Security from Concept Through Development.

One point echoed in many of these essays is the recognition that "system security engineers are first and foremost systems engineers." Susan Albert, a senior associate for system security engineering and architecture at Booz Allen Hamilton, and her colleague Jacqueline Nemeth, show security thought beginning in concept and requirements-analysis phases, and carried through in design and development phases. Susan played an active role in reviewing the symposium presentations made by the essay authors at IW09.

Balancing Security and Other Concerns within a Systems Architectural Approach

The essays in this theme section are intended to illuminate the necessarily intimate relationship of system architecture to system security. Security can neither exert a repulsive dominance over the

delivery of a system's services, nor come as an afterthought invited to the party for leftovers. Mike Wilkinson, technical director for strategy in the defense market at Atkins in the U.K., and Paul King, of Vega Consulting in the U.K., address these issues head on with a refreshing service-based approach. Mike cochairs the Systems Architecture Working Group and played an active role in reviewing all of the essays for this project and the symposium presentations made by the essay authors at IW09. His colleague, Paul has the interesting background of exploring aesthetics in enterprise architecture, a quality generally lacking in systems engineering thought processes and a glaring detriment to security engineering.

System Architecture for Managing the Nuclear Weapons Enterprise

Architecture, security, and systems engineering come together appropriately at the highest levels of conceptual system design. The security concerns of the society at large as a stakeholder are a dominant, though often slighted, factor in the nuclear weapons complex (a phrase referring to the total enterprise of nuclear weapons); these concerns supersede the functional requirements utilized in traditional engineering. Denis Engi, recently of Sandia National Labs and now with New Mexico State University, uses the nuclear weapons complex as a case study to explore a portfolio approach to integrating architecture and security where societal concerns are given first priority.

Establishing Security Strategy Using Systems Thinking

Systems thinking at its best is a state of mind. It feels and weighs all of the forces in tension, especially those generated by human activity. Applied systems thinking balances these forces in multidimensional trade space. Gifted systems engineers *live* systems thinking; gifted security engineers do, too. John Wirsbinski, as a Sandia National Labs security professional, thought it was time that systems thinking be applied to system security. John Boardman, Distinguished Professor at Stevens Institute of Technology, advised Wirsbinski's Ph.D. dissertation on the topic; their joint essay here is just a taste of that work. At the core of Wirsbinski's thinking is the idea that security engineering cannot be effective without the same broad, balanced viewpoint expected of the systems engineer. Security simply "bolted on" can only impede a system's performance. Security "woven in" is not about relocation, but rather about synergy. The Wirsbinski-Boardman essay is a fitting final bookend to Kristen Baldwin's call to arms at the beginning of the section. Both essays emphasize that security cannot succeed without the holistic viewpoint of systems engineering, and that systems cannot succeed without security engineering in the trade space.

Dedication: John Wirsbinski, 1969–2009

During the course of this INCOSE working group project my cochair and colleague, John Wirsbinski, met an untimely death in a motorcycle accident. He cofounded and cochaired the System Security Engineering Working Group, intending to make a difference. John is not able to see the budding of this work, nor the fruits anticipated from its ripening; but his leadership and thoughts give shape to it, and this work is rightfully dedicated to his memory.

John's professional attention was largely focused on security, influenced first by an internship at Idaho National Laboratories, and then in practice at Sandia National Laboratories. He worked on the physical security side, a traditional partition in today's organizations, and felt constrained. Security was something he saw in holistic terms. It is apparent that his accomplished training and teaching in martial arts shaped this point of view. Systems thinking came naturally, as did his view of security as an in-the-moment, competitive dance with an opponent. John saw an opportunity to bring all of this together with a Ph.D. path in systems engineering.

I had the privilege of collaborating with John in the attempt to realize our shared vision. His passion and tenacity were infectious and inspirational. The formation and mission of the Systems Security Working Group had a tag-team genesis: “I will, but only if you will.”

Those of us who share his vision can only carry on, inspired by his passion and his insight. Friends and colleagues have recounted the gifts he had as a human being and as a systems engineer, recognizing the loss both because of who he was and what he would have accomplished. For all the gifts he had, this series of essays and its exploration of next-generation security is the gift he leaves to all of us. In debt to his work and his passion, this theme issue of *INSIGHT* is dedicated to John.

Next Steps

The project to produce this theme section was an active beginning for the System Security Engineering Working Group. Now that we are sending these essays out into the world, we move onto an organized search and characterization of patterns that represent next-generation agile security, with the ultimate goal of establishing a body of defining artifacts. This second project is organizing as a broad, collaborative activity that will examine and analyze candidate security patterns that are resilient, proactive, adaptable, evolvable, and embraceable. We seek and welcome fellow travelers in this search, and we look forward to hosting a conference in planning now for the fall of 2010, which we intend as a defining moment for the instigation of next-generation agile security. Please contact me at rick.dove@incose.org if you would like to join our efforts.