The Buck Stops Here – System Security is a System Engineering Responsibility

Rick Dove, rick.dove@incose.org, January 2010

Current system security strategies are failing and cannot be fixed by security engineers alone. The reason for failure is evident: the "attack community" operates as an intelligent, multi-agent, self-organizing, system-of-systems, with swarm intelligence, tight learning loops, fast evolution, and dedicated intent. With few exceptions, the systems being targeted are alone, senseless and defenseless. They rely on outside benevolence for protection, whether this be separate security systems, or laws and penalties. Or they may simply think they will be overlooked by the attackers.

Intelligent attack communities range from technologically savvy guerrillas and terrorists practicing so-called 4th generation warfare against social infrastructure systems; to system hacker communities empowered by ubiquitous access to tools, techniques, and targets. In the mix we see organized crime, entrepreneurial criminals, nation-state war departments, grass-roots flash swarms, and do-it-yourself antisocial expression.

This working group believes that security engineering cannot succeed without system engineering professional attention – partly in system requirements, partly in system trade space recognition, but mainly in system thinking applied to concepts of operations and systems architecture. Sustaining system functionality in the face of intelligent determined attack requires self preservation capabilities that adapt and evolve with equal intelligence, determination, and strength of community. This requires full system awareness and adaptability, and system-of-system relationships. Security engineering alone cannot accomplish this, and what needs to be done lies at the frontier of system engineering.

Since its organizational meeting in 2007, the group has completed two projects so far, and has activated three more that will be discussed shortly. The group's roster includes approximately fifty INCOSE members who've asked for access to the membership page and documents, and a mailing list that includes an additional 15 people that are not INCOSE members—yet.

A Declaration of Responsibility

The popular phrase, *pass the buck,* denotes the passing of responsibility for a decision on to someone else. For effective security, the buck stops at systems engineering. There is nowhere else to go. This demanding situation defines our mission, articulated and published as a *Declaration of Responsibility*[1] in the INSIGHT April 2008 issue. This was the group's first completed project, and begins:

We hold these truths to be self evident,

that engineered systems are designed for purpose;
that they are engineered by their designers to meet certain fundamental requirements;
that among these are security, safety, service, and the pursuit of economic effectiveness;
that to secure these requirements design principles are instituted among the community of engineers, deriving their just nature from first principles, natural laws, and best practice;
that whenever such principles become inadequate to these ends, it is the responsibility of the community to abolish them, and to institute new principles that shall seem most likely to deliver security, safety, service, and effectiveness.

Usefully modeled after the United States' Declaration of Independence, the document goes on to justify the need for a new order that breaks with tradition, before concluding:

We, therefore, solemnly publish and declare, that the community of system engineers are, and of right ought to be, responsible for system security as a fundamental systems engineering practice, that they are absolved from all encroachment on responsibility assumed or claimed by others, and that all political and inertial

[1] Dove, Rick, and John Wirsbinski. 2008. The manifesto of the working group on systems security engineering: A declaration of responsibility. Insight 11 (2):47-49. INCOSE. www.parshift.com/Files/PsiDocs/Pap080401Insight-SecurityManifesto.pdf

connection with maintenance of the status quo be totally dissolved; and that as custodians of optimal system effectiveness they have full power and responsibility to develop principles and best practices that

employ holistic systems thinking;
assume adversary penetration of our systems always and constantly;
define and embody resilient reactive concepts;
define and embody innovative proactive concepts;
integrate all security disciplines;
embed security within system architecture;
represent meaningful measures and heuristics of risk and security effectiveness;
identify and address the realities of the environment, including human behavior, organizational behavior, technology pace, systems complexity, globalization, agile enterprise practices, and agile adversaries; and
remain both vigilant and innovative as expressions and possibilities of reality continue to change;
and to discover, define, and address all other such things which responsible systems engineers have an obligation to do.

Associating Security with System Architecture

The second completed project put a stake in the ground, tying system architecture to system security as the theme of the INSIGHT July 2009 issue. Mike Wilkinson, co-chair of the System Architecture working group, joined with us to find and review appropriate essays addressing *The Interplay of Architecture, Security, and Systems Engineering*. Table 1 displays the topics and contributors.

Table 1. Theme positioning and 11 essays published in INSIGHT, July 2009.

The Interplay of Architecture, Security, and Systems Engineering – Rick Dove	An Architecture of Information Assurance Processes – Jackson Wynn
System Security Engineering: A Critical Discipline of Systems Engineering – Kristen Baldwin	Toward a Dynamic System Architecture for Enhanced Security –Mark De Spain
Using the U.S. Department of Defense Architecture Framework to Build Security into the Lifecycle – William P. Mulokey	Balancing Security and Other Concerns within a Systems Architectural Approach – Mike Wilkinson and Paul King
Standardized Practices for Embedding Security from Concept Through Development – Susan Albert and Jacqueline Nemeth	Developing a System Architecture for Managing the Nuclear Weapons Enterprise in the Context of a Comprehensive Policy Portfolio – Dennis Engi
Resilient Control Systems: A Basis for Next-Generation Secure Architectures – Craig Rieger	Establishing Security Strategy Using Systems Thinking – John Wirsbinski and John Boardman
Secure Architecture and Design of Component-Based Systems – Karen Mercedes Goertzel	Embedding Agile Security in System Architecture – Rick Dove

Handbook and CSEP System Security Knowledge

This working group has accepted the responsibility for making sure the *Systems Engineering Handbook* and CSEP examination prepare engineers for the challenges of system security. With a sense of urgency, we are defining projects to initiate the development of knowledge appropriate for system-security segments in the handbook and the CSEP test. However, the usual methods of filtering and selecting from best practice are not available, because in the area of systemic security there is little or no practical experience to draw from directly. Therefore we also accept the responsibility to instigate the demand for, discovery, and deployment of the appropriate system engineering concepts for next-generation security. *Instigation* is the appropriate word here, as the effort must necessarily be a collaboration between the systems-engineering and security-engineering communities, spanning commercial, government, and academic interests. Three such early-stage projects are discussed next.

Patterns of Agile System Security

How will system engineering facilitate sustainable system functionality in the face of intelligent determined attack? Is there any body of practice that can help answer this question? We think so, and have established a project to illuminate appropriate architectural and operational concepts that can be used as conceptual building blocks for next-generation system security strategy. Our interest is with the security contextual aspects of system engineering, not with the details and technologies of security engineering. Our interest is also in developing a language common to system engineering and security engineering that can forge a shared working vision. We are now engaging in the first phase of the patterns project[2] depicted in Figure 1.

In this first phase we adopt an initial set of tools that are being evaluated with use and are expected to evolve with experience. The six SAREPH characteristics shown in Table 1 mirror observed characteristics of the attack communities; we have adopted these as initial filters for selecting candidate operational patterns of system security.

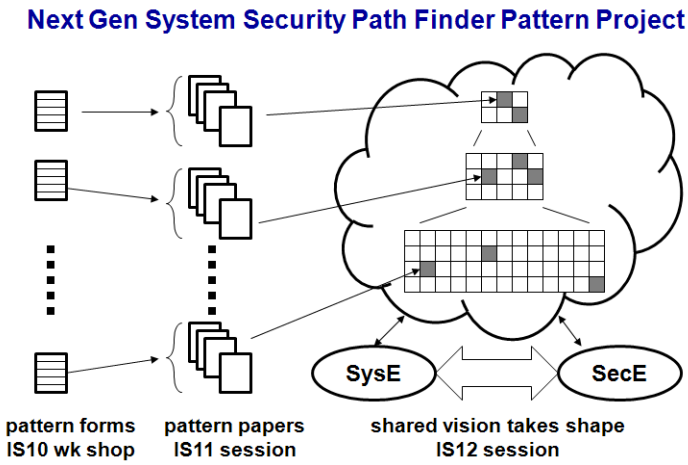

Figure 1. Three phase project plan

Table 2. Pattern qualification filters

[S] Self-organizing – with humans embedded in the loop, or with systemic mechanisms.
[A] Adapting to unpredictable situations – with reconfigurable, readily employed resources.
[R] Reactively resilient – able to continue, perhaps with reduced functionality, while recovering.
[E] Evolving with a changing environment – driven by situation and fitness evaluation.
[P] Proactively innovative – acting preemptively, perhaps unpredictably, to gain advantage.
[H] Harmonious with system purpose – aiding rather than degrading system/user productivity.

Table 3 shows the pattern "form" that is being employed initially. We reviewed a number of initial pattern-capture attempts at the 2010 International Workshop to guide subsequent work for review at another workshop at the 2010 International Symposium, and plan then to develop phase-2 papers of next-generation patterns for a session at the 2011 symposium. Phase 2 should lay groundwork for a phase-3 attempt at shaping the beginnings of a pattern language that can articulate a shared next-generation vision for systems engineers and security engineers.

Table 3: Pattern form

Name: Descriptive name for the pattern
Context: Situation that the pattern applies to
Problem: Description of the problem
Forces: Tradeoffs, value contradictions, key dynamics of tension and balance, constraints
Solution: Description of the solution
Graphic: A depiction of response dynamics
Examples: Referenced cases of pattern use
Agility: Evidence of SAREPH characteristics
References: Access to examples in literature

[2] Dove, Rick. 2009. Modeling agile next-generation security patterns. Working paper of the INCOSE System Security Engineering Working Group. www.parshift.com/Files/PsiDocs/ModelingAgileNextGenerationSecurityPatterns.pdf

The pattern form emerged from an iterative application and discovery precursor activity, which identified and described three pattern examples called Dynamic Phalanx Defense, Peer Behavior Monitoring, and Swarming Threat Sensors[3]. All three examples reference multiple supporting instances in the literature in a variety of different system domains. Figure 2 shows the pattern graphic for the Dynamic Phalanx Defense, a device of the pattern form intended to display time-based response dynamics.

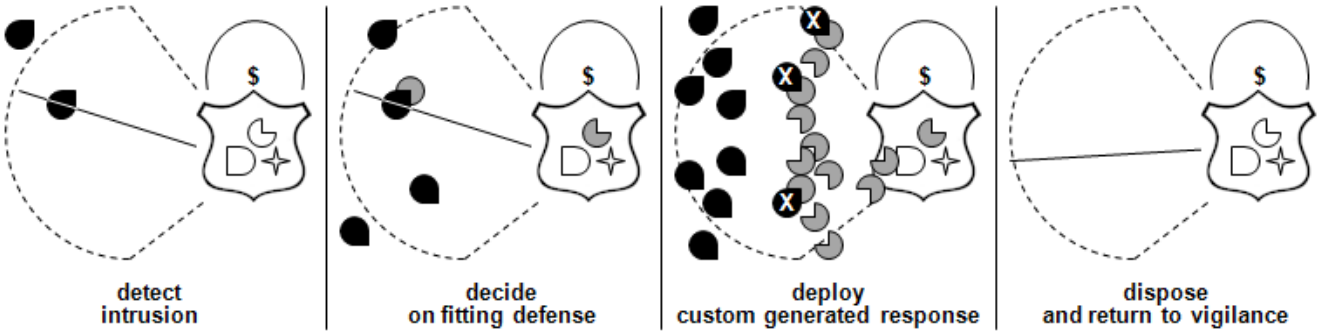

Figure 2. An aggressive shield waxes and wanes measure-for-measure in real time. Used in network Botnet defense, just-in-time drone swarms, the human immune system, and the natural chemical defense of growing plants.

Standards Affecting System Security

Standards affecting the security of systems are of particular interest to the group. Next-generation system security must effectively counter unforeseen attack methods and defend unprepared attack targets in some semblance of real time. Standards can enable or inhibit that ability at all points in the system life cycle. Standards can also be the common Achilles heel for attack vectors taking advantage of known commonality. Standards compliance can absolve design and operational responsibility for security failure. Standards can preclude unforeseen but necessary response. But standards can also establish responsibility, facilitate collective response, and enable collaborative evolution. The working group acknowledges the impact of relevant industry standards on system security; and recognizes that INCOSE has obligation to represent its membership in relevant standards activities, and to interpret for its membership the impact of relevant standards. This working group is concerned with how existing and new standards might enable or inhibit next-generation security concepts in the systems engineering context, and accepts a necessary responsibility to interpret and represent INCOSE appropriately in standards activities.

The International Organization for Standardization is starting the development of a standard for "Secure System Engineering Principles and Techniques" under the "Information Technology: Security Techniques" standards structure. This working group was contacted by Ken Crowder, INCOSE's liaison to ISO/IEC JTC 1 SC 7, in the fourth quarter of 2009 and asked to consider participation. Ironically, we had just submitted a panel abstract for the 2010 symposium entitled "Self-Organizing vs. Standards-based System-Security Strategy: Conflict or Synergy?" We agreed to be involved and work out the details at the 2010 International Workshop

Catalyzing a Shared Vision Across Communities

To wrap up our current project plans: the working group has joined with the INCOSE Enchantment Chapter in New Mexico to organize a catalytic event, with the intent of bringing together the systems-engineering and security-engineering communities around a shared working vision. Internal notice of the concept of this event was published in the October 2009 *INSIGHT*, tentatively scheduled for the fourth quarter of 2010.

Join Us at the Frontier

It is fitting for INCOSE to tackle next-generation security, as the issues are leading edge systems engineering issues: architecture, systems of systems, self-organizing systems, security tradeoffs with human factors, systems thinking. Participants in this working group's projects will be in the vanguard of systems engineering developments.

[3] Dove, Rick and Laura Shirey. 2010. On discovery and display of agile security patterns. CSER, March 17-19, Hoboken, NJ. www.parshift.com/Files/PsiDocs/Pap100317Cser-OnDiscoveryAndDisplayOfAgileSecurityPatterns.pdf