Self Organizing vs Standards-Based System-Security Strategy
Conflict or Synergy

Moderator: Rick Dove, PSI Inc., USA
Panelists: Dr. Brian White, The MITRE Corporation, USA
Kristen Baldwin, Department of Defense, USA
Ken Kepchar, FAA, USA
Rick Dove, PSI Inc., USA

Abstract

Self organizing systems-of-systems characterizes the operational architecture of the anti-system adversarial community – from guerillas and terrorists to organized computer crime, high-seas pirates, grass-roots vigilantes and independent system hackers. These anti-system communities are loosely coupled multi-agent systems bound only by shared learning loops of tools, techniques and targets. Contemporary system security strategy is failing against this intelligent operational evolution. The need for next generation security strategies is fueling early action. One avenue is crafting new standards and new acquisition requirements – another avenue is probing security structures that mirror the adversarial architectures of self-organizing systems-of-systems. The former sounds like a centralized approach, the later a decentralized approach. Is there conflict, compatibility or synergy between these two approaches?

Biographies

Moderator

Rick DOVE teaches graduate courses in agile systems and agile self-organizing systems of systems in the School of Systems and Enterprises at Stevens Institute of Technology, is Chairman of Paradigm Shift International, and a founding partner of Kennen technologies. He co-founded and chairs the INCOSE working group on Systems Security Engineering and is a board member of the New Mexico INCOSE chapter. He is author of Response Ability – The Language, Structure, and Culture of the Agile Enterprise; and Value Propositioning – Perception and Misperception in Decision Making. He has 40 years experience at start-up, turn-around, interim executive, and program management. He was co-Principle Investigator on the OSD/Navy-funded project that identified systems and enterprise agility as the principle competitive factor for the new millennium, and organized and led the DARPB/NSF-funded Agility Forum activity that did the initial industry-collaborative research on the architectural and operational characteristics of agile systems. He holds a BSEE from Carnegie Mellon University, with additional graduate work in Computer Science at U.C. Berkeley.

Panelists

Dr. Brian E. WHITE was Director of the Systems Engineering Process Office (SEPO) at The MITRE Corporation from 2003-2009. He held a Corporate position and reported to MITRE's Corporate Chief Engineer. Dr. White's current professional interests are focused on applying complexity theory and complex systems principles to improving the practice of systems engineering in situations where the interactions of people (considered part of the system) dominate the technological issues. Dr. White is founding Co-Editor of a book series established in 2007 called Complex and Enterprise Systems Engineering with Taylor & Francis. He is co-editor and chapter contributor to a book, Enterprise Systems Engineering: Theory and Practice, and co-author (with Beverly Gay McCarter) of another (draft) book entitled Leadership in Decentralized Organizations; he is co-author (with Beverly Gay McCarter) of a chapter called Emergence of SoS, Socio-Cognitive Aspects for another T&F book entitled Systems of Systems Engineering: Principles and Applications that appeared in 2009. From 2005-2008, Dr. White was the International Council on Systems Engineering (INCOSE) Assistant Director for Systems Science and the founding Chair of the Systems Science Enabler Group (SSEG). He received Ph.D. and M.S. degrees in Computer Sciences from the University of Wisconsin, and S.M. and S.B. degrees in Electrical Engineering from M.I.T. He served as an Air Force Intelligence Officer, and for 8 years was at M.I.T.'s Lincoln Laboratory. Dr. White spent 5 years as a principal engineering manager at Signatron, Inc. In his 28 years at The MITRE Corporation, he has held a variety of senior technical staff and project/resource management positions. He was MITRE's Global Grid Architecture Project Leader for four years, and worked in the fields of digital communications and networking, satellite and radio communications, and modulation/coding for many years before that. During his professional career, Dr. White has published more than 100 significant technical papers and reports.

Mrs. Kristen BALDWIN serves as Deputy Director, Software Engineering & System Assurance ODUSD(A&T)/SSE, Pentagon. She is the focal point for developing new software engineering and system assurance policies and strategies, and teaming with Components, Industry and Academia to improve DoD software development and integration process. Ms. Baldwin serves AT&L as lead for Systems of Systems (SoS) Systems Engineering guidance, Capability Maturity Model Integration (CMMI) oversight, and the Institutional Reform and Governance effort that resulted from the 2005 Quadrennial Defense Review. She has been with OSD since 1998, where she has led the application of capabilities based planning in the acquisition process, with a focus on the integration of requirements, acquisition, and programming processes; served as Deputy Director, Software Intensive Systems; and managed the Tri-Service Assessment Initiative. Prior to OSD, Ms. Baldwin served as a Science and Technology Advisor in the Army's Office of the Deputy Chief of Staff for Operations and Plans, and at the Dismounted Battlespace Battle Lab, Fort Benning, GA. Ms. Baldwin received a Bachelors degree in Mechanical Engineering from Virginia Tech in 1990 and a Masters in Systems Management from Florida Tech in 1995.

Ken KEPCHAR is the Chief Systems Engineer for Integration and Information System Security within the NextGen Integration Office of the FAA Air Traffic Organization. In this position, he is a member of the FAA Enterprise Architecture Board, and the lead instructor for System Engineering, Risk Management, Information System Security for System Engineers and Validation & Verification. Prior to that, Ken was Chief System Engineer at the FAA's Technical Center in Atlantic City. He also held several Information Security positions ddealing with communications, navigation, and surveillance systems in the FAA's National Airspace System (NAS). Ken has over 40 years of technical experience in the aviation industry, 25 of those years in management. He has held numerous positions at the Chapter and International levels of the International Council of Systems Engineering (INCOSE). He has served on the INCOSE Board of Directors and most recently as the initial Program manager and Chair of the Certification Advisory Group for the INCOSE Certified System Engineering Professional (CSEP) program. Ken holds a B.S. (aeronautics and astronautics) from the Massachusetts Institute of Technology and an M.S. (engineering management) from the University of Missouri – Rolla. Ken is a Certified System Engineering Professional (CSEP) and a registered Certified Information System Security Professional (CISSP).

Draft
7 Apr 10
B. E. White

Position Statement for INCOSE Symposium 2010 Panel
Conflict of Self Organization and Standards for Next Generation System Security Strategy
Organizer and Proposer: Rick Dove

I definitely favor the 2nd (self-organizing) approach outlined in the panel abstract. Cyber attacks are asymmetrical, and we need to respond at least in kind, taking Ashby's Law of Requisite Variety [Ashby, 1958] to heart. Think of mimicking how the human body's immune system works. Try to at least match the defensive strategies to those of the attacks—and go beyond! Endeavor to increase one's robustness health-wise to build further defensive and offensive [Harris, 2009] capabilities to counter future, as yet unspecified, unpredictable, and emergent attacks. [Dove and Shirey, 2010] We need to develop more "right-brain" holistic, conceptual, and cognitive methods for cyber problems instead of relying so heavily on "left-brain" analysis and often uninformative "data". [Pink, 2005] [Gladwell, 2005] Moreover, we should invest in more applied research, modeling and simulation—possibly utilizing virtual worlds like Second Life—and leverage of existing facilities that focus on experimentation to discover potential emergent effects of cyber attacks. The surprises that cannot even be explained after they are observed are of greatest interest.

In many venues and domain areas, even beyond cyber security, most stakeholder investors seem interested in "widgets" that may promise a path toward a "silver bullet," i.e., things that "water the eyes," as opposed to capabilities offered by broader infrastructure utilities. Unfortunately, we generally "can't speak truth to power" to call into question such shortsightedness. Some in positions of authority made earlier cyber decisions in furthering their career path or other mis-guided self-interest, as opposed to the public interest, that led to present vulnerabilities; they don't want to admit that. So they tend to minimize these threats by saying the equivalent of "Let's not scare the troops."

Decision makers often don't relate to or understand the [technical] issues. To assist them we must show them how [cyber] failures affect their missions. We need to learn how to sell ideas and make them stick [Heaths, 2007], e.g., work backwards from commanders' decisions points, getting their attention by telling them what they might not be able to do because of a particular cyber attack. Put things in context using holistic system views. Tell powerful stories [Denning, 2005] to which people can relate that will get their full attention.

In addition to the thrust of the 1st paragraph above, we can also try to influence authorities to mandate the development and adoption of new or modified standards (the 1st approach in the panel abstract) and acquisition policies that gradually change incentive structures (over time—perhaps decades—but that's O.K.) to reward results instead of perceived promises. Over the long term we should try to influence changes in the "way the world works", whereas now system fielding is often approved to meet cost and schedule without sufficient assurance that its vulnerabilities have been mitigated. Further, we should strive to develop cyber capabilities in

operational environments with users to the extent feasible, i.e., in relatively controlled situations where outcomes can be reasonable assured to be safe and "contained".

One continually hears or reads diatribes from those in high positions bemoaning the fact, but providing few details about, how many acquisition programs fail. Often the reasons cited include insufficient attention to even conventional systems engineering (SE). And they are often not even knowledgeable about or conversant with enterprise or complex systems engineering (ESE or CSE) techniques that are the antithesis of the command and control, hierarchical mentality. The latest such instance, in a long list of examples, of this counter-productive syndrome was the IEEE International Systems Conference in San Diego, 5-8 April 2010. Instead one needs to create conditions for all stakeholders—including our adversaries, whose identities continually morph—to interact vigorously in pursuing self-interests based on their incentive structures and reward systems, which will result we claim, almost *de facto*, in more robust and effective cyber designs and capabilities.

Most organizational cultures either discourage or penalize information sharing, either explicitly or implicitly, despite imperatives—unfortunately, often through only "unfunded mandates"—to do otherwise. [Jackson, 2010] [Dorobek, 2009] This even happens in our so-called "war on terror" in our post 9/11 environment. Incentives and rewards for information sharing must be made compelling enough to change risk averse behaviors acquired over a long time as a result of punishments for sharing "too much". [Hathaway, 2009]

We over-classify and overprotect far too much and for reasons other than security, mainly distrust. The reasons for this are many. For example,

- Retention of information has been commonly viewed as a source of power, and many want to protect and increase what power they already enjoy.
- Relatively few organizations or individuals welcome outside scrutiny into the bulk of their activities, particularly operational policies and procedures, but also technical methods and results, because this
    - Tends to invite unwanted criticism
    - May incentivize others to compete for sources of funding
    - May jeopardize the protection of intellectual property
- Information sharing may compromise the protection of classified information or make a network less secure in the realm of cyber security, for instance.

We should only protect what is absolutely necessary for national security, and let the rest be shared openly and deliberately. [Templeton, 2009]

Regarding personal information, many people would be surprised at how little privacy they really have when it comes to data about them that's out there. [Garfinkel, 2009] Let's not kid ourselves. Not much of anything can be truly be hidden [Carr, 2009] from a determined inquisitor, enemy, or "friend" with no conscience—and perhaps 4% of the human population fall within this latter category! [Stout, 2005] Nevertheless, the benefits of sharing in trusted cultures should be able to do wonders in overcoming adversarial advantages.

It's better to assume that our adversaries already have the sensitive information and concentrate more on how we might make it is extremely difficult for them to capitalize on it. Unrealistic and unstated assumptions must be examined and revised. [Ranum, 2009] One must assume that no

one can be trusted to cause no harm. We must devise, implement, and field mechanisms where if someone acts maliciously the damage they can inflict is severely limited. For example, force them to break a unique code for each device, not just one code to bring down a whole network. Also, one must assume that most people will vote for convenience as opposed to security. They will be lax and do careless things, albeit innocently or unintentionally. [Hernandez, 2010] Compelling rewards should also be instituted so that most people will be strongly motivated to be sensitive to and report suspicious technical anomalies or inappropriate human behaviors associated with cyber security while doing their daily jobs. More attention should be paid to social engineering to help combat human-element weaknesses, e.g., education and training to create more awareness of and protection against subtle methods for obtaining passwords, etc.

So, in summary, instead of repeating mistakes of the past in following traditional or conventional SE approaches which would just "dig the hole deeper" and cause us to fall further behind our adversaries in trying to fight cyber attacks, I advocate trying fresh complex systems approaches that can only do better in protecting our security and privacy long into the future.

References

[Ashby, 1958] Ashby, W. R., "Requisite Variety and Implications for Control of Complex Systems," *Cybernetica*, Vol. 1, No. 2, 1958, pp. 83-99

[Carr, 2009] Carr, David F., "DOD warns against the dark side of social networking," *Government Computer News*, 18 June 2009, http://gcn.com/Articles/2009/06/18/DOD-on-dark-side-of-social-networking.aspx?Page=2

[Denning, 2005] Denning, Stephen, The Leader's Guide to Storytelling: Mastering the Art and Discipline of Business Narrative, Jossey-Bass (Wiley), San Francisco, CA, 2005

[Dorobek, 2009] Dorobek, Christopher J., "The Intelligence Community Writes the Book on Collaboration," *SIGNAL Magazine* November 2009, http://www.afcea.org/signal/, http://www.afcea.org/signal/articles/anmviewer.asp?a=2113&print=yes

[Dove, 2010] Dove, Rick and Shirey, Laura, "On Discovery and Display of Agile Security Patterns," Conference on System Engineering Research. Hoboken, NJ, March 17-19, 2010. www.parshift.com/Files/PsiDocs/Pap100317Cser-OnDiscoveryAndDisplayOfAgileSecurityPatterns.pdf

[Garfinkel, 2009] Garfinkel, Simson, "Privacy Requires Security, Not Abstinence—Protecting an Inalienable Right in the Age of Facebook," Essay, *Technology Review*, July/August 2009, pp. 64-71, http://www.technologyreview.com

[Gladwell, 2005] Gladwell, M., *Blink: The Power of Thinking Without Thinking*, Little, Brown and Company, Time Warner Book Group, New York, 2005

[Harris, 2009] Harris, Shane, "The cyberwar plan, not just a defensive game," *National Journal*, nextgov—Technology and the Business of Government, 13 November 2009, http://www.nextgov.com/site_services/print_article.php?StoryID=ng_20091113_1728

[Hathaway, 2009] Hathaway, Melissa E., "Strategic Advantage: Why America Should Care About Cybersecurity," Belfer Center for Science and International Affairs, John F. Kennedy School of Government, Harvard University (Harvard Kennedy School), October 2009

[Heaths, 2007] Heath, Chip, and Dan Heath, *Made to Stick: Why Some Ideas Survive and Others Die*, Random House, New York, 2007

[Hernandez, 2010] Hernandez, Johnnie, "The human element complicates cybersecurity," *Defense Systems—Knowledge Technologies and Net-Centric Warfare*, 2 March 2010, http://defensesystems.com/Articles/2010/03/11/Industry-Perspective-1-human-side-of-cyber...

[Jackson, 2010] Jackson, William, "Lack of trust still hinders public/private security efforts," *Government Computer News*, 12 February 2010, http://gcn.com/Articles/2010/02/15/Cybereye-public-private-partnerships.aspx?p=1

[Pink, 2005] Pink, Daniel, *A Whole New Mind: Why Right-Brainers Will Rule the Future*, Riverhead Books (Penguin) New York, 2005

[Ranum, 2009] Ranum, Marcus J., "The Anatomy of Security Disasters," March, 2009, http://www.ranum.com/older-stuff.htm, http://www.ranum.com/security/computer_security/editorials/disasters/V2.pdf

[Stout, 2005] Stout, Martha, *The Sociopath Next Door*, Broadway Books (Random House), New York, 2005

[Templeton, 2009] Templeton, Hollis, "Social media benefits trump security fears," 10 June 2009, http://news.medill.northwestern.edu/washington/news.aspx?id=133987

Bio - Dr. Brian E. White was Director of the Systems Engineering Process Office (SEPO) at The MITRE Corporation from 2003-2009. He held a Corporate position and reported to MITRE's Corporate Chief Engineer. Dr. White's current professional interests are focused on applying complexity theory and complex systems principles to improving the practice of systems engineering in situations where the interactions of people (considered part of the system) dominate the technological issues. Dr. White is founding Co-Editor of a book series established in 2007 called Complex and Enterprise Systems Engineering with Taylor & Francis. He is co-editor and chapter contributor to a book, Enterprise Systems Engineering: Theory and Practice, and co-author (with Beverly Gay McCarter) of another (draft) book entitled Leadership in Decentralized Organizations; he is co-author (with Beverly Gay McCarter) of a chapter called Emergence of SoS, Socio-Cognitive Aspects for another T&F book entitled Systems of Systems Engineering: Principles and Applications that appeared in 2009. From 2005-2008, Dr. White was the International Council on Systems Engineering (INCOSE) Assistant Director for Systems

Science and the founding Chair of the Systems Science Enabler Group (SSEG). He received Ph.D. and M.S. degrees in Computer Sciences from the University of Wisconsin, and S.M. and S.B. degrees in Electrical Engineering from M.I.T. He served as an Air Force Intelligence Officer, and for 8 years was at M.I.T.'s Lincoln Laboratory. Dr. White spent 5 years as a principal engineering manager at Signatron, Inc. In his 28 years at The MITRE Corporation, he has held a variety of senior technical staff and project/resource management positions. He was MITRE's Global Grid Architecture Project Leader for four years, and worked in the fields of digital communications and networking, satellite and radio communications, and modulation/coding for many years before that. During his professional career, Dr. White has published more than 100 significant technical papers and reports.

System Security Engineering

A Standards-Based Position

Introduction

Department of Defense (DoD) systems are large-scale, complex, and interconnected. They are built by prime contractors with scores of subcontractors and suppliers, and they often consist of commercial and unique components operating side-by-side. In order for the Department to have confidence that its systems will perform only as intended, it must have a way to trust the components and processes that perform those mission-critical functions. A standards-based approach to system security engineering provides a basis for designing, developing, and testing for system security attributes throughout the lifecycle.

Commercial Standards: Buying With Confidence

Military systems' increasing dependence on commercially supplied components is driving the Department to engage with industry on acceptable standards for security and assurance. We are reaching out to industry and the International Organization for Standardization (ISO) to consider a standards-based approach that can enable confidence in our understanding of the composition of purchased components and the interactions of those components with other system elements. This is critical to foster the ability to leverage a global technology marketplace and commercial products while composing systems with confidence in assurance.

COTS components are and will continue to be integral to our military systems, networks, and support enterprise. However, we currently lack a standard for what comprises a secure commercial product. If we are able to define "goodness", commercial suppliers will have an easier time developing secure products and the Department will have a better idea of what is needed to integrate those components.

Based upon this industry outreach The Open Group has initiated a project that will:

1. Identify issues affecting the acquisition of trustworthy commercial products
2. Identify best practices in the areas of security, quality, and supply-chain management
3. Define a way forward to recognize commercial products that use those best practices.

In addition to the industry-wide standards we are pursuing, the prevalence of integrated circuits in military networks and systems is driving a specific focus on the supply chain management of information and communications technology (ICT).

A complimentary effort with substantial industry and government participation (Cisco, Microsoft, Intel, Boeing, Northrop Grumman, CSC, Booz Allen, DHS, NIST, NSA, and others) is addressing supply chain

considerations in ISO standards. This could lead to an overarching information and communications technology supply chain security standard.

Acquisition/Engineering Standards: Building with Integrity

While the Department is depending on security/assurance standards from industry at the component level, we are also pursuing broad engineering standards at the system integration and acquisition level.

A broad framework for implementing standard security controls already exists for Information Assurance – these were initially mandated by DoD policy and are now in the process of being adopted as National Institute of Standards and Technology standard. In 2003, the Department began laying a framework for implementing system security, developed a definition for system assurance, and a risk-based strategy for achieving it with Systems Engineering at the core. DoD partnered with industry to develop engineering guidance for security, and in 2008, the National Defense Industrial Association issued the Engineering for Systems Assurance guidebook.[1] This guidebook, which provides process and technology guidance to aid program managers (PMs) and systems engineers (SEs) who are seeking guidance on how to incorporate assurance measures into their system life cycles, has since been adopted by the North Atlantic Treaty Organization (NATO) Standardization Agency.[2]

The Department is also engaging in the development of an international standard for systems and software assurance, ISO/IEC 15026. This ISO standard is written for use with other life cycle standards such as 15288, *System life cycle processes*, or 12207, *Software life cycle processes*, and is meant to overlay the concepts of assurance cases and integrity levels throughout those life cycles. Part 1 of the standard has already been submitted to ISO for publication as a technical report, and the remaining Parts are in various stages of draft.

Still, there is more do be done. The Department is seeking methods, processes, and tools for Systems Security Engineering. One of the current activities is focused on identifying critical information and components in military systems and protecting them at levels commensurate with the risk of their compromise. A working group is currently studying Criticality Analysis (identifying those system components providing mission-critical functionality) so that countermeasures can be cost-effectively applied to the most important system elements. These processes will be standardized in policy and guidance Issuances.

A related activity at the Systems Engineering Research Center (SERC) is developing a research roadmap for system security engineering. The goal of the research is to establish the fundamental science and rigor in this key discipline of systems engineering, similar to the work that has been done in other

[1] National Defense Industrial Association (NDIA) System Assurance Committee. 2008. Engineering for System Assurance. Arlington, VA: NDIA.

[2] ENGINEERING FOR SYSTEM ASSURANCE IN NATO PROGRAMMES. AEP-67, Edition 1. February 2010.

specialty disciplines (e.g. Safety, Reliability). The SERC hosted a workshop from March 31-April 1, 2010 to gather industry and academia input on the direction of this roadmap.

Way Ahead

The complex, interconnected nature of DoD systems necessitates standards-based approaches to system security engineering. At the component level, the Department is working with industry to develop commercially acceptable standards for assuring integrity. At the acquisition and integration level, current activities are elevating system security as another specialty discipline of systems engineering so that security concerns are considered early and often throughout the acquisition lifecycle. More work is needed to advance this standards-based approach to acknowledge complex, highly networked systems and systems-of-systems assurance.

Moving forward, forums like the INCOSE System Security Working Group provide the Department with an opportunity to share intent and progress, as well as to learn from practitioners across a variety of industries. The Department will rely on Systems Engineers to consider security in the design trade space such that our critical information, technology, and functionality are protected cost-effectively.

Bio - Mrs. Kristen Baldwin serves as Deputy Director, Software Engineering & System Assurance ODUSD(A&T)/SSE, Pentagon. She is the focal point for developing new software engineering and system assurance policies and strategies, and teaming with Components, Industry and Academia to improve DoD software development and integration process. Ms. Baldwin serves AT&L as lead for Systems of Systems (SoS) Systems Engineering guidance, Capability Maturity Model Integration (CMMI) oversight, and the Institutional Reform and Governance effort that resulted from the 2005 Quadrennial Defense Review. She has been with OSD since 1998, where she has led the application of capabilities based planning in the acquisition process, with a focus on the integration of requirements, acquisition, and programming processes; served as Deputy Director, Software Intensive Systems; and managed the Tri-Service Assessment Initiative. Prior to OSD, Ms. Baldwin served as a Science and Technology Advisor in the Army's Office of the Deputy Chief of Staff for Operations and Plans, and at the Dismounted Battlespace Battle Lab, Fort Benning, GA. Ms. Baldwin received a Bachelors degree in Mechanical Engineering from Virginia Tech in 1990 and a Masters in Systems Management from Florida Tech in 1995.

Panel Position:

Critical infrastructure is a term to describe (physical) assets that are essential for the functioning of a society and economy – usually grouped into sectors:

Transportation	Telecommunications
Power	Financial services
Energy	Water
Food	Public Health
Security	Governmental services

The US Government has invested heavily to safeguard its information systems and networks, especially those elements that comprise its "critical infrastructure". This was in response to the Federal Information Security Management Act (FISMA), which requires compliance with specific regulations and standards, both present and emerging.

Recently, there is a growing recognition in government circles that logical IT network capability is as critical and vulnerable as the physical - effectively an extension of ´critical infrastructure "from physical to the logical domain. As a fundamental principle, cyberspace is viewed as a vital asset for the nation and the United States should protect it using all instruments of national power, in order to ensure national security, public safety, economic prosperity, and the delivery of critical services to the American public.

This shift in viewpoint has generated considerable interest and debate on the role of government AND the private sector in protecting our IT capabilities. Proposed legislation in the US Congress directly addresses this issue, and in part says: "President Obama has … determined that 'our digital infrastructure - the networks and computers we depend on every day will be treated . . . as a strategic national asset'. With more than 85 percent of the Nation's critical infrastructure owned and operated by the private sector, it is vital that the public and private sectors cooperate to protect this strategic national asset."[1] While most of the IT capability that our nation's economy depends on lies in private hands, there is no consistent sets of standards and rules to guide the development, deployment, and operations of this vast mosaic.

Much of our current and emerging government network capability can be classified as a widely distributed Systems-of-Systems (SoS). They are composed of multiple complex systems functioning independently, but at the same time are federated to deliver overall capabilities and services. An example can be taken from my background – aviation. Air Traffic Management in this country is handled by the FAA using the National Airspace System (NAS), which is US government critical infrastructure. It is composed of systems that are ground-based, airborne, and space-based. They effectively work together to provide the communications, navigation, and surveillance necessary to safely and efficiently transit our airspace.

[1] Committee Amendment dated 3/10/10 to S. 773 - Cyber Security Bill of 2010

Today's cyber environment exhibits the following characteristics– accelerating complexity and unprecedented connectivity in a hostile environment of increasing sophistication and scale that threatens to overwhelm the resources of the most robust system or network. Quality of service, data integrity, ability to operate in a compromised environment, situational awareness and response are objectives that all IT owners and operators struggle to provide. Couch those business objectives in terms of "critical infrastructure" and interoperability become as important a consideration. Interoperability must occur at multiple levels:

- International
- Federal
- State
- Private sector

Going back to my aviation example, a substantial portion of our commercial flights are regional or global in nature. That means, that they transit national boundaries, and their systems must be capable to communicating with different Air Traffic Management infrastructure internationally. Likewise, airports in this country are owned and operated by a jurisdiction below the federal level, which requires interoperability as the flight transits from one airport to another. Finally, the avionics and systems used on our modern aircraft are produced by the private sector. Even though designs are different, the installed systems still need to operate interchangeably. All this reinforces that standards are not only needed, they are essential to an efficient and effective SoS.

While the US Government moves to protect its networks and information, the private sector has not been under the same mandates, even in regulated industries. Consequently, private entities are free to implement safeguards and technologies that best fit their situation and business model. The individual entities that make up today's System of Systems are networked to a degree that risks are shared across these networks. This lack of standardization allows for interfaces between networks across the public-private divide to be exploited and provide an asymmetric attack vector to negate the safeguards that have been built into public critical infrastructure systems. The example from aviation that comes to mind is the aircraft interacting with the (ground-based) Air Traffic Management system. As aircraft design becomes more and more digitally based, how can we effectively ensure that protection mechanisms for airborne systems and ground systems are compatible and mutually supportive?

Standards are often consensus based and slow – especially in comparison to a market-based technology innovation cycle. This disparity does not argue for standards as an impediment to innovation; rather, it argues that the standards need to be performance based rather than technology based, and allow the innovation to occur in the application of the standards.

Networking interdependency and complexity extends to the organizational context itself through "the diversity of stakeholders associated with (this endeavor). The most daunting challenge in the development and deployment of widely distributed SoS is the massive coordination effort among the various stakeholders and the synchronization of activities to both deliver benefits and efficiencies and provide common assurance to all parts of the enterprise. Stakeholder groups will likely differ in viewpoint, which will be reflected in the needs and requirements. This

diversity must be effectively managed, most likely through a collaborative governance process, in order for (the endeavor) to be successful.

The US Government has recognized both the benefits and vulnerabilities of a federated approach to System of Systems and networks. However, today's interconnectivity and blurring of system boundaries demand an unprecedented level of collaboration and cooperation to secure the IT infrastructure involved. More sophisticated and higher threat levels warrant increased interoperability and coordination, something that can only be achieved in a standards-based context. The question before this panel amounts to how private systems that interact with critical infrastructure can offer the assurances required to protect the integrity of critical infrastructure networks and data. In other words how can each of us effectively shift our mindset from a system view to an enterprise view of risk management while preserving our ability to innovate and compete in the open market.

Biography:

Ken Kepchar is the Chief Systems Engineer for Integration and Information System Security within the NextGen Integration Office of the FAA Air Traffic Organization. In this position, he is a member of the FAA Technical Review Board, which is the technical arm of the NAS Enterprise Architecture Board. He is the lead instructor for System Engineering, Risk Management, and Information System Security for System Engineers within the FAA. Ken has over 40 years of technical experience in the aviation industry, 25 of those years in management.

Ken has held numerous positions at the Chapter and International levels of the International Council of Systems Engineering (INCOSE). He has served on the INCOSE Board of Directors and recently as the initial Program manager and Chair of the Certification Advisory Group for the INCOSE Certified System Engineering Professional (CSEP) program.

Ken holds a B.S. (Aeronautics and Astronautics) from the Massachusetts Institute of Technology and an M.S. (Engineering Management) from the University of Missouri – Rolla. Ken is an INCOSE Expert System Engineering Professional (ESEP) and a registered Certified Information System Security Professional (CISSP).

Next Generation Security Needs Next Generation Standards

Panel Position Statement For:
Self Organizing vs Standards-Based System-Security Strategy - Conflict or Synergy

Rick Dove, dove@parshift.com

The reality of standards is impeding system security. If things continue as they have, system security will only get worse.

Current system security strategies are failing because attack communities operate as 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 – relying on outside benevolence to protect them, whether that be third party security systems, laws and penalties, adherence to security standards, or perceived probabilities of being an overlooked target.

These 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 systems targeted by organized crime, entrepreneurial criminals, nation-states, grass-roots multi-agent swarms, and independent back-yard system hackers.

These attack communities are diverse in nature and allegiance, but draw strength from at least six shared agile-system characteristics:

- Self-organizing – with humans embedded in the loop, or with systemic mechanisms.
- Adapting to unpredictable situations – with reconfigurable, readily employed resources.
- Evolving in concert with an ever changing environment – driven by vigilant awareness.
- Resilient in reactive response – able to continue, perhaps with reduced functionality, while recovering.
- Innovative with proactive initiative – acting preemptively, perhaps unpredictably, to gain advantage.
- Harmonious operations – aiding rather than degrading attack-system functional productivity.

To provide parity with the agility of intelligent attacking systems, security mirroring the agile attack community's six characteristics seems minimally necessary. Prima facie, self organizing attack systems are thriving in large measure, and they emerged without the benefit of central planning, engineering design, or enforced standards.

Self organization among system agents requires interoperability – common interaction protocols and methods as a minimum. What are the standards that facilitate the operational effectiveness of the adversarial community? It is clear that they are minimal, they evolve and emerge, they are voluntary but so beneficial that adoption need not be "required", and they have been highly effective.

At least two architectural concepts providing interoperability standards for self organizing attack communities are evident: publish-subscribe and service oriented architecture (SOA). Publish-subscribe simply makes use of the web as infrastructure for access to rapidly-evolving information on tools, techniques, and targets; and is employed by self-sufficient agents. SOA also relies on the web, but in this case it is employed to stitch together momentary supply-chain networks where individual agents provide specialty services employed in an overall attack.

In contrast is the reality of standards employed by defenders. They require formal consensus, take the force of contract, are slow to develop and slow to change. They are too often employed as a lazy means to demonstrate best practice and sufficient diligence, but in fact provide CYA proof that alleviates the need to put real security

first. This is not an indictment of security engineers or operational security forces, but rather the decision makers in management and acquisition that define sufficiency and constrain resources.

If self-organized systems-of-system concepts are to be employed as a defense strategy, standards need to facilitate and enable the formation and operation of security communities promoting innovation, evolution, and cross-domain learning equal to the attack communities, as a minimum.

To put the situation in perspective, the technology of weaponized unmanned autonomous systems is advancing in cycle times of only a few months. Traditional test and evaluation (T&E) procedures take many months and more. As a result, T&E is being ignored by the war fighter. Removing a human from harms way or dealing effectively with a tough threat takes precedence. New weapon capabilities are tested first in the field under fire by the people who need them now. Security standards that impede the needs for rapid innovation and constant evolution will invite the same disrespect, and risk becoming road kill.

Rapid innovation and constant evolution cannot happen without interoperability standards, but these must be kept to a minimum or they begin to constrain rather than enable. The standards we have and the standards we add are examples of evolving systems and eco-systems in their own right – adding elements to improve robustness over time. Studies of system-evolution fundamentals, both biological [1] and technological [2], show that system evolution is driven by the need for robustness, is accomplished by increasing system complexity, and is accompanied by increased system fragility.

In the words of Carl Woese [1]: “Vertically generated and horizontally acquired variation could be viewed as the yin and the yang of the evolutionary process. Vertically generated variation is necessarily highly restricted in character; it amounts to variations on a lineage’s existing cellular themes. Horizontal transfer, on the other hand, can call on the diversity of the entire biosphere, molecules and systems that have evolved under all manner of conditions, in a great variety of different cellular environments. Thus, horizontally derived variation is the major, if not the sole, evolutionary source of true innovation.”

Woese’s simulations have shown that Darwinian vertical evolution does not converge on optimal solutions, whereas horizontal evolution is driven toward it. As cellular systems evolved more complexity, they eventually crossed what Woese calls the Darwinian threshold, where the preservation and strengthening of internal component dependences becomes favored over the innovative but more risky incorporation of outside components. Now cast this understanding into the evolving ecology of security standards, not moving toward optimal solutions, but rather protecting and institutionalizing previous best practices.

Horizontal and vertical system-evolution interplay is a new understanding hidden in plain site—and discovered by another team from a different angle: highly optimized tolerance, a very HOT idea.

Jean Carlson and John Doyle understand something about complex systems and the way they age that provides strong theoretical underpinnings for the behaviors observed in complex systems ranging from the Internet to the Immune system—and the growing complexity of the security standards ecological system.

In theirwords [2]: “Through design and evolution, HOT systems achieve rare structured states which are robust to perturbations they were designed to handle, yet fragile to unexpected perturbations and design flaws. As the sophistication of these systems is increased, engineers encounter a series of tradeoffs between greater productivity or throughput and the possibility of catastrophic failure. Such robustness tradeoffs are central properties of the complex systems which arise in biology and engineering.”

Adding robustness initially or incrementally over time creates complexity within the system, preserving and protecting its essential functions and capabilities against known uncertainties. But at the same time, the system becomes increasingly fragile to unexpected threats and so-called Black Swans—unavoidably.

Highly readable and targeted at the systems engineer, Woese, Carlson, and Doyle back-to-back is the stuff of naked insight. A deafening click! There is small utility in just letting this explain the world around us. It should be put to work in purposeful design.

Increased system fragility is the antithesis of increased system security.

It is time for a standard for responsive standards, for real-time self-organizing standards, and for a systems view of the dynamics of the standards eco-system that can illuminate the trade off of robustness for fragility [3]. As a panel debating position the way forward for these three paths is not the focus, for the need to move must first be understood.

References

1. Woese, Carl. 2000. Interpreting the universal phylogenetic tree. PNAS. 97(15):8392-6. www.ncbi.nlm.nih.gov/pmc/articles/PMC26958/pdf/pq008392.pdf
2. Doyle, J.C., Low, S., Carlson, J.M., Paganini, F., Vinnicombe, G., Willinger, W., and Parillo, P. 2005. Robustness and the internet: Theoretical foundations. in Robust Design: A Repertoire of Biological, Ecological, and Engineering Case Studies (Santa Fe Institute Studies on the Sciences of Complexity), Eric Jen, Editor, Oxford University Press. http://gabriel.physics.ucsb.edu/~complex/pubs/SFI_Networks_2005.pdf
3. Bayuk, Jennifer. 2010. The utility of Security standards. proceedings SERC Security Workshop, March 31 – April 1, Washington D.C.

Bio - Rick Dove teaches graduate courses in agile systems and agile self-organizing systems of systems in the School of Systems and Enterprises at Stevens Institute of Technology, is Chairman of Paradigm Shift International, and is a founding partner of Kennen Technologies. He co-founded and chairs the INCOSE working group on Systems Security Engineering, and is a board member of the New Mexico INCOSE chapter. He is author of *Response Ability – The Language, Structure, and Culture of the Agile Enterprise*; and *Value Propositioning – Perception and Misperception in Decision Making*. He has 40 years experience at start-up, turn-around, interim executive, and program management. He was co-Principle Investigator on the OSD/Navy-funded project that identified systems and enterprise agility as the principle competitive factor for the new millennium, and organized and led the DARPA/NSF-funded Agility Forum activity that did the initial industry-collaborative research on the architectural and operational characteristics of agile systems. He holds a BSEE from Carnegie Mellon University, with additional graduate work in Computer Science at U.C. Berkeley.