

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 their words [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.