Embedding Agile Security in System Architecture

Rick Dove, rick.dove@incose.org

In Abraham Maslow's five-level hierarchy of needs (Maslow 1943), the first level is physiological (air, food, water, etc) and the second is safety (the security of knowing that physiological needs will be satisfied). In Maslow's theory, a person can attend to subsequent needs at higher levels only after satisfying these first two levels, and only to the extent that excess attention and resource is available. This concept makes intuitive sense to all of us. We can relate to it very personally. It also used to make sense to the "proto-systems-engineers" of earlier centuries, in the days when the major systems were fortress towns, standing armies, tribal alliances, and protected food and water sources. But the continued development of civilization and technology created leisure and room for self-indulgence. We've built systems to serve us in all manner of purpose, unconcerned with the lessons of history. Over time we've marched into a *cul de sac*.

Now we are feeling the impact of self organizing "anti-systems," designed to exploit, repurpose, consume, and destroy. At the core of these anti-systems are technically adept humans wielding technology with malevolent intent. Nation states are developing and exercising the ability to disrupt the economic and infrastructure systems of other nation states. Technically sophisticated criminals have built a thriving marketplace for tools and resources aimed at financial and economic system intervention. Warfare methods now characterized as fourth generation (Robb 2007) pit small guerilla units against nation states effectively, with rapidly evolving do it yourself weaponry and strategies aimed at economic and infrastructure systems. And at the scary extreme are individuals now technologically empowered to intervene and disrupt DNA-system targets, should they wish. All of these anti-systems have the advantage of intelligent self-organization, more degrees of freedom than their targets, and the initiative to adapt and evolve rapidly.

Defining the Characteristics of Next-Generation Security

Current-generation security is characterized principally as reactive: it is invented and deployed in response to the escalating sophistication of attack experiences. As an after-the-fact defense insertion, it is typically an add-on functional subsystem, force-fit to the system that needs protection.

In contrast, next-generation security is an emergent property of the system it protects. To provide parity with the agility of intelligent attacking systems, six characteristics are needed:

- self-organizing,
- adapting to unpredictable situations,
- evolving in concert with an ever changing environment,
- reactively resilient,
- proactively innovative, and
- harmonious with system purpose.

These six characteristics occur at three levels: self-organization is the top "umbrella" level, since adaptation and evolution are themselves self-organizing processes; resilience, innovation, and harmony are the values delivered by the processes. These six characteristics are the foundation of an agile ability to respond – to opportunity as well as to threat – and form the core of a *response-able* system architecture.

Self-Organization

In my research and teaching I have come to understand agile systems as self-organizing, though often not in the sense that comes immediately to mind. I divide agile systems into two classes: class 1 contains *reconfigurable* agile systems, which include embedded people that perform the organizing functions; class 2 contains *reconfiguring* agile systems, which have systemic mechanisms that accomplish these functions. In both cases these systems are in a constant state of self-organization in response to opportunity and threat. If these functions cease, the system is no longer agile.

Adaptability

When an agile system is confronted with a novel situation, it will reorganize its resources in a configuration appropriate to the situation. Adaptability is enabled by an inventory, or immediate acquisition, of appropriate resources. Typically adaptation is what occurs in tactical time frames, and is a real-time response to an opportunity or threat. When the situation allows time for a response, adaptation may include some modification of existing or available resources, provided that the new resource version is compatible with the overall system. Adaptation includes the use of existing available resources in new ways and for new ends.

Evolvability

Evolution takes time to develop new strategic avenues of capability, but don't think of it in biological time frames, slow by "nature." Think rather of John Boyd's OODA loop (observe-orient-decide-act) concept and the need to cycle your evolutionary learning loops faster and tighter than your adversary does (Boyd 1976; Hammonds 2002). Boyd's OODA loop is typically thought of as a tactical concept, more akin to competitive adaptability during adversarial engagement, but his fundamental model and the origins of the concept are based on cross-generation evolution of knowledge patterns (Boyd 1992).

Reactive Resilience

Agile systems live effectively in a world of risk, prepared to recover from disruptive incidents. The term *resilience* as a systems characteristic has origins in ecological systems, where fires, drought, hurricanes, construction runoff and other such insults disrupt a smoothly functioning ecological system. Ecological resilience allows the absorption of a shock that may alter the affected system for a while, but the system eventually returns to vibrant functionality. The phrase *survivable systems* is used in computer science, in general conformance with the concept of shock absorption and a possible period of performance degradation, but of course in a much faster time frame.

The immune system is a good role model of a self-organizing, resilient response process: it swings into action when an attack occurs and mounts an aggressive defense. A successful first-time defense learns from experience and is usually able to absorb subsequent attacks of the same nature with little or no performance degradation. Research in the new field of artificial immune systems is advancing quickly and has already resulted in new approaches to intrusion detection products (Forrest and Hofmeyr 2001).

Proactive Innovation

The term *proactive* deserves careful attention, since it is often misused. The word came to prominence in (Frankl 1959), a translation from the original German used to describe people who take responsibility for their own lives, rather than seeing their life as a reaction shaped in response to outside forces or other people. Stephen Covey, crediting Frankl, is probably responsible for the present popularity of the term, designating *Be Proactive* as the first of his *Seven Habits of Highly Effective People* (Covey 2004: 65-94). Marketers quickly seized on this term, with its positive connotation, and pressed it into service selling products, often independent of the meanings cited here. Today people frequently misuse the term to simply mean active as opposed to passive. One way to know if someone is using the term *proactive* correctly is to ask whether the person is using it to mean an initiative (one that makes other people become reactive) and/or an innovation (something both novel and valuable).

An excellent discourse on proactive security in the face of aggressive engagement is John Boyd's classic, but unpublished, eight-page essay from 1976, "Destruction and Creation."

Harmonious (Embraceable, Invisible)

If a system's security mechanisms are not harmonious with the objectives of the people who use the system, they are not sustainable. Too much of the security effort these days is an imposition on user productivity. The effect is willful user rebellion, with too-frequent disregard and compromise of security policies, practices, and processes. If security compliance is tough and comes with a personal cost, willful compromise will occur, as well as unintended mistakes.

Natural systems have evolved examples of harmonious security: the immune system, for instance, doesn't maintain an infection-fighting population of antibodies on patrol until they are needed. Human designed systems have also addressed this need: for instance, making fire-retardant glass every bit as beautiful and transparent as regular glass encourages people to use the fire-retardant type when appropriate. Harmony is a common design principle in construction architecture but not in system architecture—a topic worth exploring at another time.

Depicting Response-Able Architecture

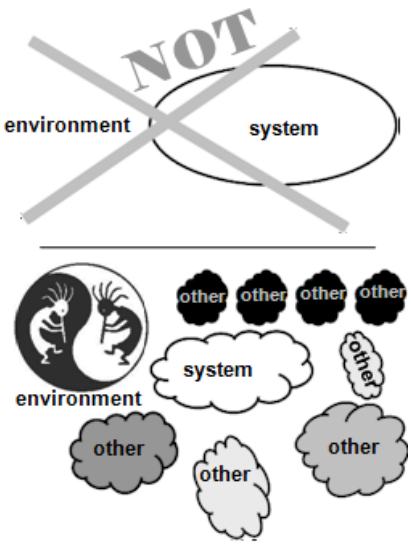

Figure 1. Like Kokopelli, the trickster of Hopi lore, the environment dances to its own tune, accelerating the beat in a dynamic ecology of competition and aggression.

The typical "blob diagram" shown at the top of figure 1 depicts a system inside a static boundary and everything else outside. We call that everything else the environment. This is badly misleading. Systems are situated, but they are not alone in the environment, and the environment is not benign.

Think back to your teen years. Commissioning a system is like going to a dance—in another part of town. The environment is the music. Dancing alone does nothing but advertise presence. Real dancing is with others, some in partnership, more in challenge, all in self-gratification. When the music changes, different moves are needed. When performance escalates, a matching response is needed. When others lead, graceful following is necessary. Better to lead and let others stumble catching up, or enrapt them with an unparalleled display. The music never stops, it just changes.

Adaptation is an immediate, appropriate, different response in functionality. This can only occur if functional resources can be added, modified, or reconfigured quickly. A good sports team has more players than it fields at any one time, so that the coach can mix and match the players' skill-sets according to the opposition, the situation, and real-time developments.

Reconfiguring a sports team with different players during game time doesn't work, though, if players bring their own rules with them. The players all know the rules of the game and they all know their team's playbook. The coach exercises a drag-and-drop, plug-and-play operational strategy enabled by an actively managed team-system structure. Complex system behaviors arise from the interactions of simple rules. Were this not the case, it would be impossible to sustain complex behavior in the face of increased opportunities for failure.

"Response-able" systems (Dove and Turkington 2009), as depicted in figure 2, have the following characteristics:

1. resource pools to draw upon when system reconfiguration is needed,
2. a passive infrastructure that enables and constrains synergistic interoperation, and
3. an active infrastructure of governance composed of four processes for tending and evolving systems.

System tending and evolution encompass four generic processes. These processes must be actively staffed (class 1) or systemically automated (class 2), or else a potentially agile system loses integrity and becomes prey or roadkill. Response ability is enabled by structure, and sustained by active control.

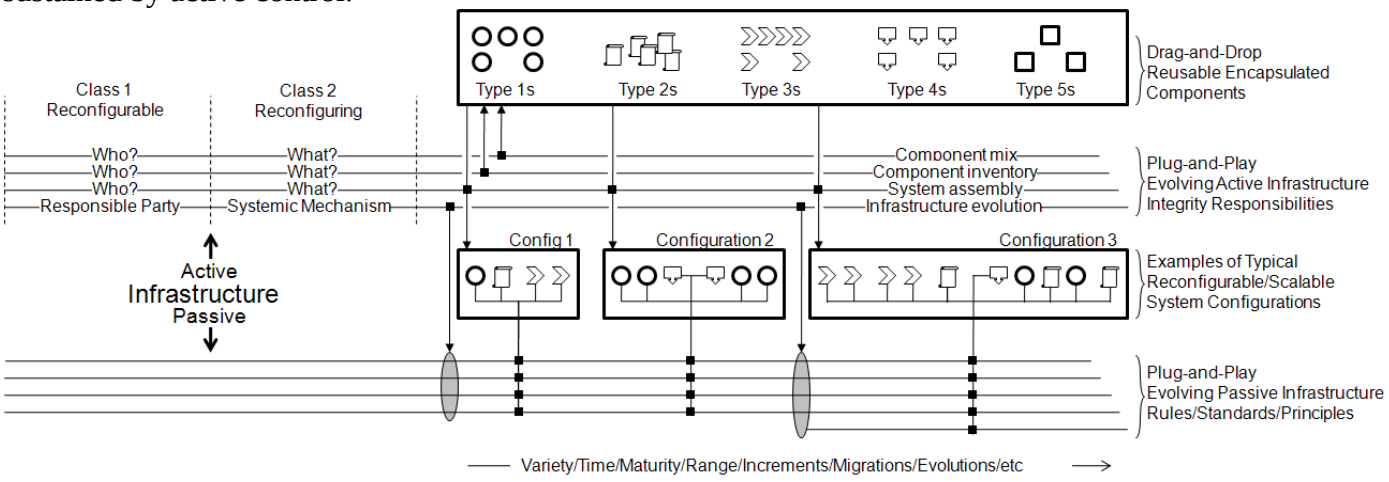

Figure 2. Generic drag-and-drop/plug-and-play architectural pattern for class 1 and class 2 "response-able" systems. This architecture often suits component subsystems as well.

I've referred to this active control as the portion of infrastructure that performs governance. You can also think of it as an intelligent control subsystem at the core of the larger system. Today this intelligence is generally provided by humans as an integral part of the system. An extreme but illustrative example includes all the humans involved in operating, repairing, upgrading, and defending today's sophisticated military naval vessel.

Embedding Security in "Response-Able" Architecture

Figure 3 shows a stylized architectural concept for a next generation multi-range weapons testing system, one that can test new weapon systems and subsystems quickly by reconfiguring and augmenting modular components. As a next-generation capability, this test system will have to deal with unmanned autonomous systems (UAS) working together in heterogeneous, multi-agent systems of systems. Testing intelligent autonomous systems bring a new dimension to security concerned with intelligent attackers. These intelligent systems undergoing test may themselves become intelligent attackers, threatening the testing system as well as the surrounding environment. Whatever the cause for aberrant behavior, the consequences can be intolerable. The evolution of the testing systems must keep pace, as a minimum, with the evolution of UAS technology.

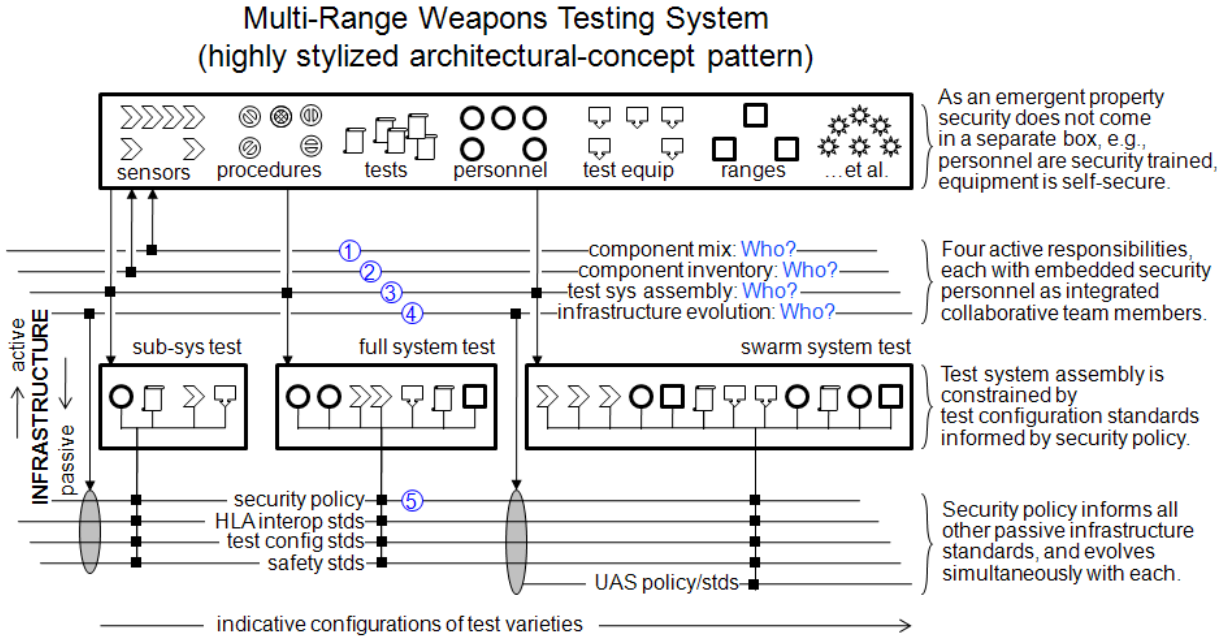

Figure 3. Security is embedded in architecture at points 1-5. Additionally, encapsulated components have internal security distrustful of other components in general, ideally a fractal image of this architecture.

The architectural structure depicted in figures 2 and 3 is fundamentally present in all systems that exhibit sustainable adaptation and evolution. In figure 3, the four horizontal lines numbered 1, 2, 3, and 4 represent the self-organizing active part of the infrastructure. If any of these four functional responsibilities are omitted from the system design, or become inactive during system operation, the vulnerability of the system increases precipitously. Describing these four responsibilities:

- Component mix – is the active responsibility to have a requisite variety of components matched to ever-changing situational possibilities. This is the function that provides adaptability. Designated persons or processes must upgrade and add

new component capabilities before their absence would compromise effective system response.

- Component inventory – is the active responsibility to enable an appropriate and timely reconfiguration of system capabilities, and is a function of the presence and condition of component inventory.
- System assembly – is the active responsibility to reconfigure the system in response to a new need. This might be a network security administrator changing the network topology, or the immune system accelerating the growth of appropriate antibodies.
- Infrastructure evolution – is the active responsibility to extend the operational portion of the system's lifecycle into new generations of proficient response. For the passive portion of infrastructure, evolution modifies the standards, rules, and policies which constrain and enable component interoperability. For the active portion of infrastructure, evolution modifies the people and processes that carry out these four active responsibilities of self organization.

System response ability is necessary but not sufficient for secure systems. The architecture shown in figure 3 enables only the "act" part of John Boyd's OODA loop. Agile next generation secure systems must also be aware (observe), conclusive (orient), and decisive (decide) in choosing a response option. These latter three are the situational knowledge-management aspects that drive response-able self organization.

References

Boyd, J. 1976. Destruction and creation. Unpublished paper. www.scribd.com/doc/12627002/Destruction-and-Creation-by-John-Boyd.

———. 1992. A discourse on winning and loosing. Unpublished paper. Abstract and first of five parts available at www.d-n-i.net/boyd/pdf/intro.pdf.

Covey, S. 2004. *The 7 habits of highly effective people: Restoring the character ethic*. New York: Free Press. Originally published (New York: Simon & Shuster, 1989).

Dove, R. 2001. *Response ability: The language, structure, and culture of the agile enterprise*, New York: Wiley.

Dove, R., and G. Turkington. 2009. On how agile systems gracefully migrate across next-generation life cycle boundaries. *Global Journal of Flexible Systems Management* 10 (1): 17–26. Available at www.parshift.com/Files/PsiDocs/Pap080614GloGift08-LifeCycleMigration.pdf.

Forrest, S., and S. Hofmeyr. 2001. Engineering an immune system. *Graft* 4 (5): 5–9. Available at http://www.cs.unm.edu/~forrest/publications/EIS.pdf.

Frankl, V. 1959. *Man's search for meaning: An introduction to logotherapy.* Translated by Ilse Lasch. Boston: Beacon Press. Originally published in German as *Ein Psychologe erlebt das Konzentrationslager* (Vienna: Verlag für Jugend und Volk, 1946).

Hammonds, K. H. 2002. The strategy of the fighter pilot. *Fast Company* 59 (June), http://www.fastcompany.com/magazine/59/pilot.html.

Maslow, A. H. 1943. A theory of human motivation. *Psychological Review* 50 (4): 370–96. Available at http://psychclassics.yorku.ca/Maslow/motivation.htm.

Robb, John. 2007. Brave New War – The Next Stage of Terrorism and the End of Globalization. New York: Wiley.