SERC Security Workshop on New Approaches to Security Engineering

Washington D.C., March 31-April1, 2010

Illuminating Next Generation Patterns of Agile System Security

Rick Dove, rick.dove@parshift.com
Paradigm Shift International
Box 289, Questa, NM 87556
575-586-1536

Illuminating Next Generation Patterns of Agile System Security
Rick Dove, Paradigm Shift International

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 – relying on outside benevolence for protection, whether this be separate security systems, laws and penalties, or perceived probabilities of being an overlooked target. Here we address the workshop's first concern, and define next generation security as co-evolving in this arms race with systemic self-organization that leverages community at least equally agile to the adversary in six observed common characteristics: self organization, adaptable tactics, reactive resilience, evolvable strategies, proactive innovation, and harmonious operations.

Operating as self-organizing systems-of-systems, 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 Internet 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. Attack communities are diverse in nature and allegiance, but their strength is rooted in six common characteristics generally absent in current system security strategy. In a word, the adversary is agile.

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 begun a research 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.

The growing body of work in patterns for system architectures has inspired a pattern descriptive approach arising from reviews of Christopher Alexander's seminal construction-architecture pattern work (Alexander 1977), and many others that have adapted the pattern concept to other fields. Our interest is focused on developing a pattern language that can be common and meaningful to both system engineers and security engineers, and comfortably informative to decision makers.

Stephanie Forrest (Forrest et al. 1994) is a pioneer in adapting lessons from biology to security strategies. Though her focus tends to be on cybersecurity, her insights seem appropriate to a much wider class of systems.

> *"Among the principles of living systems we see as most important to the development of robust software systems are: Modularity, autonomy, redundancy, adaptability, distribution, diversity, and use of disposable components."* (Forrest et al. 2005)

Life adapts and evolves, it is resilient, it is innovative, and it is in harmony with its environment. Lessons from the sustained evolution of species would seem appropriate for consideration in agile security design. Well known are the threat-responsive swarming behaviors exhibited by ants and bees, where large numbers of simple units work together to drive off or eliminate the threat. As individual units they only understand a simple common immediate goal and follow basic rules to achievement. Social animal life exhibits built-in systemic mechanisms for detecting security-threatening behavior among its members, and mitigating that behavior if it is evaluated as intolerable. Peer behavior policing is evident in humans (Myers 2008), animals (Flack et al. 2006) and insect societies (Heinze 2003).

Without much difficulty early spot-examples of self organized system security can be found. Society evolved police forces only in the last 150 years, and relied on self-organized peer behavior monitoring for most of history. Interestingly, current police theory is moving back toward community policing concepts as being more responsive and custom fit to the neighborhood needs. Ad hoc mesh networks are addressing issues of self policing among nodes. Unmanned autonomous vehicle research is facing issues of peer-peer abnormality detection. Some plants exhibit abilities to detect insect attacks and emit selected gasses that call in the appropriate insect predators. Collective cyber-intrusion incident response communities are emerging among some organizations with similar characteristics. Of special note, there is a considerable body of work in artificial immune systems (AIS) applied to security. Just to name a few.

A self organized group of volunteers who work at the intersection of systems and security engineering, with representatives from academia, intelligence, defense, and commercial interests, is now engaged in the first phase of the patterns project depicted in Figure 1. This first phase adopts 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 key observed characteristics of the attack communities, and are adopted as initial filters for selecting candidate operational patterns of next generation system security.

Table 1: 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 vigilant situation and fitness evaluation.
[P] Proactively innovative – acting preemptively, perhaps unpredictably, to gain advantage.
[H] Harmonious with system purpose – aiding rather than degrading system and user productivity.

In the work conducted to date we have used these six 'rough' SAREPH characteristics as filters for selecting candidate agile security techniques – though no research conclusions guide us yet for suggesting how many or what combinations might be minimally necessary, or even if these six are sufficient.

Figure 2 shows the initial pattern "form" populated with an early example pattern. The research plan includes a Phase 1 review of a number of initial pattern-capture attempts with a small group of volunteer pattern developers mid-year 2010, and then advancing those that show most promise into a Phase 2 set of pattern-specific papers that should lay groundwork for a Phase 3 attempt at shaping the beginnings of a multi-level pattern language. The purpose of the pattern language is to demystify the concepts of self-organizing systems-of-systems as a system security foundation, and to open working relationships between systems engineers, security engineers, and decision makers.

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 . 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.

Research into the nature of SAREPH characteristics manifested in the adversary communities should offer a deeper foundation for exploring and developing similar architectures and operational modes, and perhaps point the way to superior capabilities through purposeful system engineering.

Pattern languages have pattern hierarchies. Christopher Alexander's work, for instance, recognizes towns, buildings, and construction as successively nested pattern categories. In the course of selecting and developing initial test examples, like the one shown in Figure 2, it became evident that all were middle level patterns, and that at least a three level hierarchy would be appropriate. A lower level set might encompass patterns within individual agents that enable and compel their participation in multi-agent system-of-system patterns like that in Figure 2. A higher level set might encompass patterns of governance, autocatalysis, behavior attractors, and evolution drivers. Some questions to answer include: Are three levels sufficient or are there more to be explored, and how is a level bounded? Alexander arrived at 253 patterns he felt sufficient to capture the principle concepts of his field of interest, but then his field has eons of practice and maturity. It will likely be some time before the bounds and structures of self-organizing systems-of-systems reveal themselves.

Recognizing patterns in security strategies, identifying those that are agile, and defining them in a reusable pattern format can help accelerate the inclusion of agile security as part of the systems engineering process. This work intends to develop a population of "path finder" patterns of agile security, expecting they will be replaced with a more historical-based pattern compendium once sufficient experience is accumulated on the way toward a mature "pattern language". This initial work should provide a platform for subsequent study and augmentation.

References

Alexander, Christopher, *A Pattern Language: Towns, Buildings, Construction*, Oxford University Press, 1977.

Dixon, Colin, Anderson, Thomas and Krishnamurthy, Arvind, Phalanx: Withstanding Multimillion-Node Botnets, NSDI'08: Proceedings of the 5th USENIX Symposium on Networked Systems Design and Implementation, April 2008.

Dove, Rick. 2009. Embedding Agile Security in System Architecture. *Insight* 12 (2): 14-17. International Council on Systems Engineering, July. www.parshift.com/Files/PsiDocs/Pap090701Incose-EmbeddingAgileSecurityInSystemArchitecture.pdf

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

Edge, Kenneth S., Gary B. Lamont, and Richard A. Raines, Multi-Objective Mobile Network Anomaly Intrusion, International Journal of Computer Science and Network Security, 6(3b):187-192, March, 2006.

Flack, J. C., Girvan, M., de Waal, F. B. M. and Krakauer1, D. C., Policing Stabilizes Construction of Social Niches in Primates, *Nature*, 439 (7075): 426-429, 2006.

Forrest, S., Perelson, A. S., Allen, L., and Cherukuri, R., Self-Nonself Discrimination in a Computer, In Proceedings IEEE Symposium on Research in Security and Privacy, Oakland, CA., May 16–18, 1994.

Forrest, S., Balthrop, J., Glickman, M. and Ackley, D.. K. Park and W. Willins Eds. *The Internet as a Large-Scale Complex System*, Oxford University Press, 2005.

Hambling, Dave, Drone Swarm for Maximum Harm, Defense Tech. April 10, 2006. http://defensetech.org/2006/04/10/drone-swarm-for-maximum-harm/

Heinze, Jürgen, Reproductive Conflict in Insect Societies, In *Advances in the Study of Behavior*, ed. P. Slater, and J. Rosenblatt, 34: 1-57. New York: Academic Press, 2003.

Mahimkar, A. , Dange, J., Shmatikov, V., Vin, H. and Zhang, Y., dFence: Transparent Network-Based Denial of Service Mitigation, in Proceedings of 4th USENIX Symposium on Networked Systems Design and Implementation (NSDI 2007), Cambridge, MA, April, 2007.

Myers, David, Play and Punishment: The Sad and Curious Case of Twixt, In Proceedings of The [Player] Conference, August 26-29, Copenhagen, Denmark, 2008.

Wilkinson, Sophie, Plants to Bugs: Buzz Off!, Chemical and Engineering News, June 30, 2001.

Zhang, C., Zhang, J., Liu, S., and Liu, Y., Network Intrusion Active Defense Model Based on Artificial Immune System. Fourth International Conference on Natural Computation, Jinan, China, October 18-20, 2008.

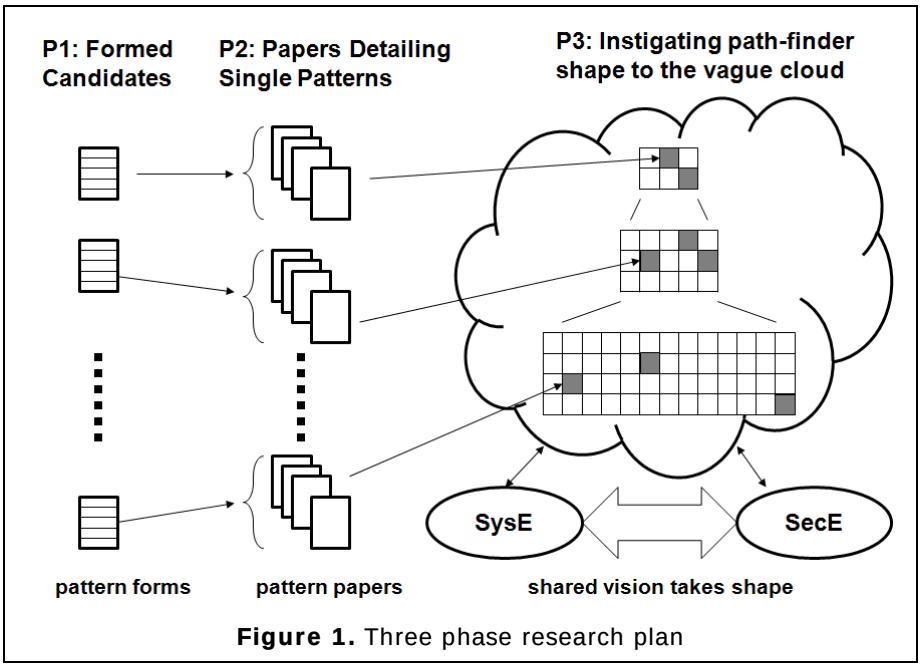


Figure 1. Three phase research plan

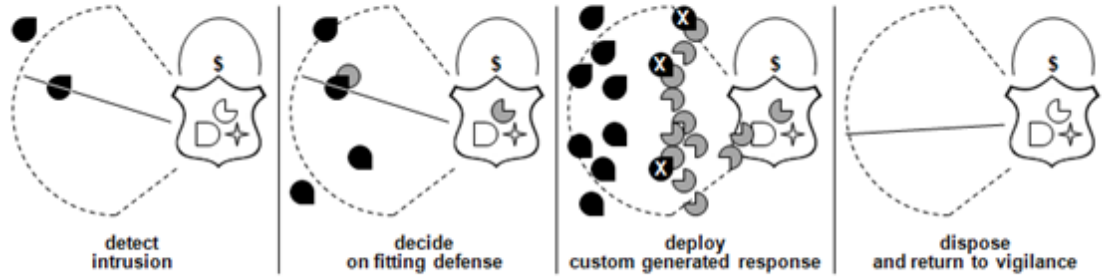
Name: Dynamic Phalanx Defense

Context: a stationary or mobile asset subject to unpredictable swarm attacks.

Problem: Attackers can come in many and unpredictable forms, and in virtually unbounded quantities, with no advance warning. For instance, A DDoS attack on an Internet service node may be of many different types; an attack on a naval asset may be surface, undersea or air in many different varieties.

Forces: Resilience of service vs. cost of service. Comprehensive counter capability and capacity vs cost and disharmony of a broad standing counter force.

Solution: the ability to detect the threat and the nature of its attack, the ability to produce and deploy appropriate disposable counter-measures, the ability to deploy measure-for-measure and to stand down or dispose of deployed counter measures when the threat is vanquished.



Aggressive shield waxes and wanes measure-for-measure in real time

Example: Artificial immune system – detection, selection, cloning and retirement applied to mobile network intrusion detection and repulsion. See (Edge et al. 2006, Zhang et al. 2008).

Example: Botnet denial of service defense – Instantly recruit an unbounded network of computers to shield a server from being overwhelmed by botnets. See (Dixon et al. 2008, Mahimkar et al. 2007).

Example: Just-in-time drone swarms – Load disposable drones with modular sensor and weapon choices, and deploy quantities as needed. See SWARM, JITSA discussion in (Hambling 2006).

Example: Plant chemical defense – Insect saliva triggers selective toxic gene expression and gas emissions that call in selective insect predators.,

Agility: Self organization grows and shrinks a counter swarm in measured response to an attack swarm. Adaptability selects appropriate counter-swarm agents from modular resources. Resilience is exhibited with expendable and replicable counter agents, and in continued operation of the protected asset, though perhaps at reduced performance. The process is harmonious with protected asset functionality as it is only activated upon detecting a threat, and then only in dynamic measure-for-measure as needed. [S-A-R-H]

References: (see reference section, only URL shown here, all accessed 30Nov09)

- (Dixon et al. 2008) www.cs.washington.edu/homes/ckd/phalanx.pdf.
- (Edge et al. 2006) http://paper.ijcsns.org/07_book/200603/200603C08.pdf
- (Hambling 2006) http://defensetech.org/2006/04/10/drone-swarm-for-maximum-harm/
- (Mahimkar et al. 2007) www.cs.utexas.edu/~yzhang/papers/dfence-nsdi07.pdf
- (Wilkinson 2001) http://pubs.acs.org/cen/critter/plantsbugs.html
- (Zhang et al. 2008) www.computer.org/portal/web/csdl/doi/10.1109/ICNC.2008.782

Figure 2. Example of a pattern description synopsis. As these descriptions are for path-finder patterns rather than of well-known common-practice patterns, full understanding is either obtained from reading the referenced papers or from reading accompanying discussion pages.