Biologically Inspired Cyber Defense and Cloud Computing Techniques
Position Paper for Safe in the Clouds Workshop

Michael Atighetchi, Partha Pal, Rick Schantz
Raytheon BBN Technologies, Cambridge MA
February 7, 2011

1. Introduction

Biological metaphors in cyber security have been around for quite some time, starting early with the naming of emerging threats (viruses, worms), and continuing with recent new and large R&D programs like DARPA CRASH that combines a “clean slate” approach to underlying infrastructure with a focus on adaptive system behavior to achieve immunity and resilience. Technologies being developed under the CRASH program are geared to preventing an information system from falling victim of cyber attack (innate immunity), facilitating faster recovery if the attack succeeds in causing some level of failure, and preventing future instances of the same attack to achieve the same level of success (adaptive immunity). Similarly, while the roots of Cloud Computing can be traced back to the early days of high-performance computing and remote access time sharing systems, recent advances in commoditizing computing power and storage capacity are unveiling new opportunities. In this extended abstract we outline our experiences in developing adaptive cyber defense capabilities that aim to achieve high level of survivability by using the adaptive immunity metaphor as key. And just like biological systems that need to survive in a cooperative, natural environment beyond their immediate complete control, so too digital technologies need to effectively operate in an environment that the users may not own nor directly control. While that environment should foster cooperative actions crossing boundaries of self, ownership and control, it also needs to effectively deal with not such cooperative behavior, and downright detrimental behavior, as well. We conclude with our view of how adaptive cyber defense approaches and operating within the paradigm shift outsourcing computation and storage to 3rd party resources may be mutually beneficial and influence each other.

2. Biologically Inspired Cyber Defense

Adaptivity is a key to survival in both nature and in information systems. We have been experimenting with applying adaptation to information system security and survivability issues for many years. Early DARPA work (APOD [1] and ITU [2]) focused on identifying anomalous behavior and utilizing redundancy management techniques to orchestrate adapting to the anomaly: undesired changes caused by attacks were healed by using alternates. In addition, it introduced techniques to make system responses less completely predictable, an early version of introducing changes into a system, somewhat analogous to compatible mutation, so that the changed system does not fall victim to the same attack. We have progressed from using low level and automatic (fast reacting) control strategies to more analytic and systematic cognitive control loops (CSISM [3]) where we can apply reasoning toward situation assessment and selection of responses. In a biological metaphor, this would be a simple attempt to attach intelligent behavior (brain functions) to drive and interpret sensory and regulatory
components of an overall autonomous entity, albeit in a digital information sense. Experimentation here focused on the degree to which these reconfiguration decisions under duress (attack) could be made without operator intervention.

From there, our latest incarnation, A3 (for Advanced Adaptive Application environment) tries to use and couple adaptive behavior across the spectrum of attributes normally associated with a biological immune system—packing and integrating adaptations for resistance/protection, immediate recovery from anomalous symptoms, and acquired immunity against specific and successful attacks. Although the techniques used are tailored to the specific needs and context from information system constructs, they notionally try to parallel the epochs and operation of biological disease fighting. Working within the confines of the DARPA CRASH program, we will have the opportunity to tie these “close to the application” adaptations with system infrastructure (environmental) improvements that are derived from taking a clean slate starting point to more fundamental components such as hardware protection combined with new operating system and programming support for providing a better operating environment for the adaptive applications. This clean slate approach to infrastructure development can be thought of as environmental cleanup to promote a more “healthy” environment to operate by replacing items which have proven to be potent breeding grounds for information system disease and infection.

3. Cloud Computing Issues

The trends in cloud computing, whichever definition you choose, keep expanding the options and improving the economics of highly interconnected but dispersed environments. At the same time it focuses attention to and further complicates some of the issues associated with making proper tradeoffs between the need to share and the need to protect information. There are two relevant R&D themes we have been pursuing related to this area. One of these focuses on federation of independent information systems with respect to smoothly but controllably combining their assets in the context of advanced middleware frameworks based on the publish/subscribe information management paradigm, managing quality of service across federated elements, and generally providing resource management and security operations effectively across and within federated elements. The other is a close cousin to this but focuses more narrowly on the issues of security mechanisms and policies for information sharing and control in a cross-domain organizational environment.

The diversity of cloud computing environments brings forth another level of heterogeneity to manage within any federation overlay for enterprise scale capabilities. This is especially obvious and crucial when it concerns quality of service and real-time behavior implications. While in the early stages of adoption these are not of primary concern, historical perspective suggests that the sharing and combining aspects across cloud instantiations will not be far behind. And in the highly competitive landscape pushing into this space it would seem inevitable to be faced with islands of useful and successful implementations, focusing more on constraining rather than expanding the boundaries of controlled federated sharing. In such an environment the cross domain issues and approaches take on even more importance. Not only do we have the traditional geographic separation and varying sharing goals and objectives of the cooperating organizations as significant domain boundaries, we introduce additional layers of ownership
and service provider domain crossing focused more on privacy concerns. While the relevant cross domain technology development is still in its early stages, we can see the push into new forms and new requirements with cloud computing going mainstream and commercial.


We can certainly see value and opportunity in combining these two perspectives going forward. In our view information systems which routinely and as a matter of standard design practice operate safely but adaptively to their changing environment needs to become the norm. While we still experiment with the value proposition of the specific adaptations, the “safely” partsloom large and unaddressed. As well, in a computing environment world that continues to enable better connectivity, more outsourcing, and demand for cooperative action, our technical solutions to controllably, effortlessly, and safely operating across domain boundaries remains in primitive forms, with compatibility, assurance and changeability achieved with great effort, great cost or great limitations (or all three). So while these two dimensions each have considerable agendas going forward without additional complications, we can begin to speculate about requirements and opportunities for their mutual influence and benefit.

At the requirements level, if adaptive systems become the norm, these adaptations will need to operate over more cross domain boundaries, with considerations of these boundaries and their means for safely crossing fed into the adaptation machinery. Similarly, as more cloud computing offerings take hold, we would anticipate that the same pressures and opportunities to move from static to dynamic strategies will be pushed into first the individual cloud environments and then across those environments.

At a more detailed level we see opportunity for the following cross-over themes as part of an evolving R&D agenda in these areas:

- Can the “cloud” help in supporting new adaptive defenses? It certainly has the potential to offer new and diverse resources cheaply and on demand. However, if there is not yet an adequate basis for entrusting the resources with critical computation and data and the adaptive control mechanisms that might operate both within and across clouds are largely absent..
- Can successful biology help suggest a safer and more efficient use of cloud? Biological metaphors certainly apply. A biological organism consists of diverse systems with multi-modal communication in an immersive environment – not unlike the situation facilitated by the cloud, but successful biological systems have enormous levels of tolerance and isolation, missing from current cloud incarnations.
- Can agile systems that can live in the wild be constructed safely, without waiting for aeons of time for evolution to get it right? While assurance arguments for single adaptive defenses may be quite feasible, the layering of multiple defenses can easily lead to unforeseen bad interactions – not unlike algorithms that need to be analyzed for type safety and race conditions.
