SECURITY AS IMMUNITY IN VIRTUAL ORGANIZATIONS

Elpida S. Tzafestas
Institute of Communication and Computer Systems
National Technical University of Athens
Athens 15773, GREECE
brensham@softlab.ece.ntua.gr

We are addressing the class of virtual organizations where an entrepreneurial or other activity acts as an interface between a number of existing remote services or applications and a number of customers that should interact with them in complex ways. For example, such activities include private e-Government middle services that specialize in carrying out complex tasks with many different state administration services, or commercial houses specializing in centralizing and organizing large complicated orders that involve a number of different vendors scattered around the electronic world. Because the integrated services/applications are remote and external to the middle entity responsible for the organization, the current practice is to manage the customer tasks mostly manually or in conventional ways, such as calling external entities and negotiating prices and delivery delays.

The INFRAWEBS[1] framework is being designed and developed with the vision to help business people build composite applications that tackle much of this interaction complexity as automatically as possible, with the role of human intervention not necessarily being fully dismissed. Such virtual organizations are characterized by operational and performance criteria that are independent and even sometimes incompatible with those of individual components (external services/applications) involved. This parallels the organization of multi-cellular biological organisms where the integrity of the organism as a whole is defined differently than for each of its constituent cells, and indeed many individually effective functionalities may be harmful from a systemic point of view, such as for example tumor cells, parasites etc. Because of this property, it is expected that an artificial immune system can be designed to treat integrity issues in the same way that a natural immune system does so within a multi-cellular organism.

This setup assumes that individual security problems are tackled by the corresponding components themselves, so that at the composite (organismal) level only those attacks can be identified and tackled that have functional consequences for the overall system. For instance, a component may be unavailable, or it may reply with unusual information and so on. Such dysfunctions should be detected and handled at the application level, wherever possible.

Because such distributed organizations are to be dynamic by nature, it makes sense to avoid as much as possible predefined "rigid" security schemes between components and allow plasticity, in the sense that some of the used components may later become obsolete and abandoned, or new ones will have to be included in the organization's repertoire, or the connection pathways through the virtual organization will change and so on. That is, much of the S&P testing should be designed to happen at runtime. Furthermore, individual protection schemes of existing components will be bound to change without notice. Such virtual organizations should rely on this information as little as possible.

[1] www.infrawebs.org

In such a democratic framework, that uses external uncontrollable components in a non-exclusive manner, some components may be occasionally busy or committed elsewhere. Furthermore, some external components may be occasionally updated or adapted. In this context, the exact relations between components, both structural and semantic, are dynamic and thus sometimes unforeseen.

As a consequence, it makes no sense to regard components as safe or unsafe, which is the usual approach in classical ICT security research. Instead, the same component may behave safely or unsafely for the overall organization (and even for itself) according to internal state, specifics of the requests processed, timings etc. This means that the communication channel between components cannot be assigned a unique forever-constant value of safe or unsafe; instead, the specifics of a request or message in relation with the internals of the receiver service may determine, sometimes not uniquely, whether the particular communication act is safe or unsafe. The same message may be therefore considered safe in one context and unsafe in another one. The security problem can be formulated now as a problem of managing information about information, i.e. information about message from component to component and is therefore declarative, in the sense of understanding abstract relations and flow.

Because of the above, our approach focuses on the detailed examination of exchanged messages with components to identify potential threats and only a little if any explicit component authentication is necessary. This approach sets itself in the trend of information flow regulation at runtime.

The artificial immune system is defined as a security “shell” that constitutes the control system for the autonomous virtual organization and filters incoming and outcoming information to external components or other types of active resources. This shell functions in parallel with the regular activities of the virtual organization and is responsible for recognizing hostile resources, i.e. resources that are malicious, malfunctioning or just slow. Attacks and insecure cases such as unavailability, improper treatment, unacceptability of communicated information, denial of service etc. can in principle be smoothly integrated in this configuration.

The operation of the artificial immune system mirrors exactly that of the natural immune system of first order. The natural immune system recognizes and attacks alien bodies by not allowing them to be metabolized by the body of the organism. In the same way, the security shell recognizes and captures alien or suspect messages before they are processed by the organization. A population of specialized artificial cells (that correspond to the antibodies), are triggered by the presence of the alien message and proliferate very rapidly and only as much as necessary to ensure clobbering of the alien population. Certainly, under certain conditions, for example when the alien attack is extremely severe or when there are multiple attacks concurrently, the immune system occupies a large amount of the resources of the central organization and as a result the latter is hindered in its normal operation. In nature, advanced organisms, such as vertebrates, possess also a second order level of operation, in which the population of the antibodies records information from past experience, i.e. alien body features or “templates” used for identification, so as to make resistance automatic the next time the same threat appears.

The immune systems approach proposed is in principle independent of the actual implementation of the individual components and their potential security policies. Thus, in principle, the immune algorithms are application-independent and relatively generic. But since the exact details and parameters of the algorithms need to be identified and tuned based on the case studies, it would be unrealistic to claim that the particular structure of the immune security shell would be directly applicable (“pluggable”) to other frameworks or to other

types of organization. Instead, the solution sought should be thought of as one instance of the class of solutions supported by this system in general.

Because of these, and in accordance with the usual approach in complex systems research, we have decided to study the properties of the immune system and the details of the algorithms in simulation. We are in the process of developing special purpose tools that co-develop with the simulations and the experimental design activity.

The virtual organization (the body) is a highly connected network of representations or "images" of external components (somatic cells), where for each link a "preference degree" or "degree of trust" is present. This metric is continuously monitored and updated by the security shell, according to the immune algorithm. While particular details are bound to be case-specific, in general the immune algorithm has the following properties :

- The artificial immune network regulates input-output flow between component images.
- The immune network consists of a number of nodes ("cells" or "antibodies"), each responding to one type of component message. Types are to be defined within the scope of particular applications, but as a general rule they use actual component properties or metrics. Two general-purpose antibody classes are price-related ones (e.g. "price > 100" or "price between 80 and 120") and delay-related ones (e.g. "delay < 3h").
- Many such different types have to be present and/or generated for the algorithm to work properly. For example, in the above case many variants of the type "price > X" have to be present and/or generated for different values of X. The types correspond to the biological notion of **specificity**.
- The algorithm relies on emergent population effects, hence a number of clones for each antibody should be present at any moment.
- The antibodies (clones) compete with each other for message "consumption" that leads to proliferation. The antibodies that dominate in the competition define which messages are discarded. The competition corresponds to the biological notion of **clonal selection**.
- The competition criterion is **organization-specific** and integrates both absolute global properties (for example, an antibody that executes once, is faster next time) and inter-component properties (a message not confirmed by the recipient virtual node may be weaker next time).

Future research issues include stability study of the network, extension to a two-level vertebrate-like memoriful immune system and hooking to real-world S&P policies.

References

Bersini, H. (1999). The Endogenous Double Plasticity of the Immune Network and the Inspiration to be drawn for Engineering Artifacts. In "Artificial Immune Systems and Their Applications", Springer Verlag, pp.22 – 44.

Dasgupta, D., Gonzalez, F. (2005). Artificial Immune Systems in Intrusion Detection, Chapter 7 in the book "Enhancing Computer Security with Smart Technology" by V. Rao Vemuri (Ed.), pages 165-208, Auerbach Publications, November 2005.

Goldenberg, J., Shavitt, Y., Shir, E., Solomon, S. (2005). Distributive immunization of networks against viruses using the 'honey-pot' architecture, *Nature*, December 2005.

Perelson, A., Weisbuch, G. (1997). Immunology for physicists, *Review of Modern Physics*, 69(4):1219-1267.