Experimenting with innate immunity

Jamie Twycross (jptcs.nott.ac.uk) and Uwe Aickelin (uxacs.nott.ac.uk)

Abstract

`libtissue` is a software system for implementing and testing AIS algorithms on real-world computer security problems. AIS algorithms are implemented as a collection of cells, antigen and signals interacting within a tissue compartment. Input data to the tissue comes in the form of realtime events generated by sensors monitoring a system under surveillance, and cells are actively able to affect the monitored system through response mechanisms. `libtissue` is being used by researchers on a project at the University of Nottingham to explore the application of a range of immune-inspired algorithms to problems in intrusion detection. This talk describes the architecture and design of *`libtissue`*, along with the implementation of a simple algorithm and its application to a computer security problem.

1 Introduction

One of the achievements of immunology over the last decade has been the uncovering of the innate immune system as of central important both as the initiator and the director of immune system processes Germain (2004). Artificial immune systems are beginning to take inspiration from this work and attempt to model some aspects of innate immunity. In Twycross and Aickelin (2005), the authors presented a conceptual framework for innate immunity. The framework highlighted a number of key general properties observed in the biological innate and adaptive immune systems, and discussed how such properties might be instantiated in artificial systems. The next logical step was to take these ideas and build a software system with which systems with these properties could be experimentally evaluated. This talks reports the progress made in taking that step.

2 Innate immunity

The authors have discussed innate immunity from a biological perspective in detail in Twycross and Aickelin (2005) and it is only briefly reviewed here. Cells are the principal actors in the immune system. Many immune system cells have access to their environment on two levels: the level of antigen and the level of signals. Antigen are the markers by which the immune system senses the structure of its environment. The structure is tightly coupled to the context of the environment, which is reflected by levels of signals. Perhaps it is too strong to say that a different structure always implies a different function, since there is almost certainly some duplication of function, but generally the immune system seems to follow this principle. Signals reflect what entities are doing on a higher level than antigen, which reflect what entities are doing on a structural level.

Almost all immune processes involve the interaction of groups of different types of cell. The type of a cell is really a label for its phenotypical and functional characteristics. The following characteristics were chosen as initial areas of experimental study: antigen processing, signal processing, cell binding, antigen matching and antigen response. The reasons for choosing these have already been discussed at detail in Twycross and Aickelin (2005).

3 Implementing innate immunity

`libtissue` is a software system which allows researchers to model and experiment with novel AIS algorithms and to apply them to realtime computer security problems. It is specifically designed to explore the characteristics of innate immunity described in the previous section. An AIS algorithm is implemented as a collection of cells, antigen and signals interacting within a tissue compartment. While designed for computer security problems in the first case, its design has been kept general with a view to applying it to realtime problems from other domains.

`libtissue` has a client/server architecture pictured in Figure 1. The AIS algorithm is implemented as a *`libtissue`* *server*, while *`libtissue`* *clients* provide input data to the algorithm and provide response mechanisms. This client/server architecture separates data collection by the *`libtissue`* clients

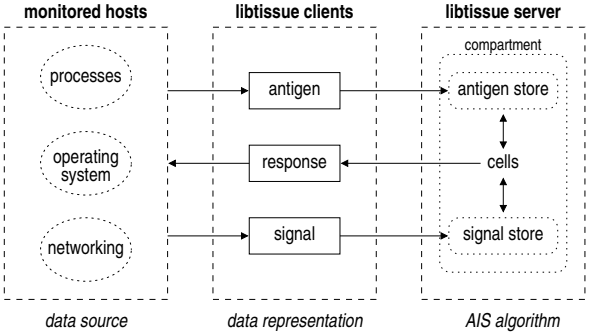

Figure 1: The architecture of *libtissue*. Hosts are monitored by *libtissue* antigen and signal clients, which in turn provide input data to the AIS algorithm, implemented as a *libtissue* server. Algorithms are able to change the state of the monitored hosts through response clients.

from data processing by the *libtissue* servers and allows for relatively easy extensibility of the existing system to new data sources. Client and server APIs exist, allowing new antigen and signal sources to be easily added to *libtissue* servers, and the testing of the same algorithm with a number of different data sources. Client/server communication is socket-based, allowing clients and servers to potentially run on separate machines, for example a signal client may in fact be a remote network monitor.

4 An example algorithm

A relatively simple AIS algorithm was implemented to validate *libtissue* and to illustrate how *libtissue* can be used to explore the behaviour of an artificial system on a realworld problem. This example has cells of two types, labelled type 1 and 2, and is shown in Figure 2. Type 1 cells are designed to emulate two key characteristics of biological APC cells: antigen and signal processing. In order to process antigen, each type 1 cell is equipped with a number of antigen receptors and producers. A cytokine receptor allows type 1 cells to respond to the value of an external signal. Type 2 cells emulate three of the characteristics of biological T cells: cellular binding, antigen matching, and response to antigen. To accomplish this, each type 2 cell has a number of cell receptors specific for type 1 cells, VR receptors to match antigen, and a response producer which is triggered when antigen is matched.

A tissue compartment is created and populated with a number of type 1 and 2 cells. The tissue compartment also stores antigen and signals received

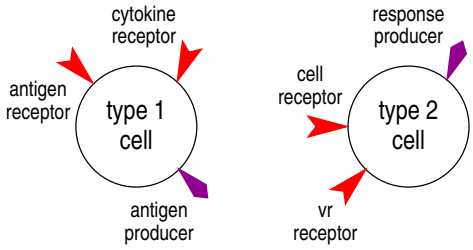

Figure 2: An example two-cell *libtissue* algorithm.

from *libtissue* clients, which provides the input data to the system. Type 1 cells ingest antigen through their antigen receptors and present it on their antigen producers. The period for which the antigen is presented is determined by a signal read by a cytokine receptor on these cells. Type 2 cells attempt to bind with type 1 cells via their cell receptors. If bound, VR receptors on these cells interact with antigen producers on the bound type 1 cell. If an exact match between a VR receptor lock and antigen producer key occurs, the response producer on type 2 cells produces a response.

5 Results

A number of experiments were carried out with the example algorithm on a realistic computer security problem, that of detecting anomalous process behaviour. The aim of these experiments was to validate *libtissue* and to highlight the methodology employed when attempting to understand the behaviour of algorithms implemented with *libtissue*. These experiments produced many interesting results, which will be presented in this talk.

Acknowledgments

This research is supported by the EPSRC (GR/S47809/01).

References

R N Germain. An innately interesting decade of research in immunology. *Nature Medicine*, 10(12): 1307–1320, 2004.

Jamie Twycross and Uwe Aickelin. Towards a conceptual framework for innate immunity. In *Proc. of the 4th International Conference on Artificial Immune Systems*, Banff, Canada, 2005.