ABSTRACT

The immune system provides a rich metaphor for computer security: anomaly detection that works in nature should work for machines. However, early artificial immune system approaches for computer security had only limited success. Arguably, this was due to these artificial systems being based on too simplistic a view of the immune system. We present here a second generation artificial immune system for process anomaly detection. It improves on earlier systems by having different artificial cell types that process information. Following detailed information about how to build such second generation systems, we find that communication between cells types is key to performance. Through realistic testing and validation, we show that second generation artificial immune systems are capable of anomaly detection beyond generic system policies. The chapter concludes with a discussion and outline of the next steps in this exciting area of computer security.

INTRODUCTION

The work discussed here is motivated by a broad interest in biologically-inspired approaches to computer security, particularly in immune-inspired approaches to intrusion detection. The first part of this chapter gives a brief overview of biologically-inspired computing and computer security, and introduces the field of artificial immune systems. We have developed an immune-inspired process anomaly detection system. Process anomaly detection is an important technique in computer security for detecting a range of attacks, and the second part of this chapter introduces and reviews current approaches to process anomaly detection, relating our work to other work in this area. The third section of this chapter introduces our own efforts to develop a prototype immune-inspired realtime process anomaly detection system. However, our interests are also wider, and address issues concerning how artificial immune systems are modelled and implemented in general. We have implemented a system, libtissue, in which immune-inspired algorithms can be developed and tested on real-world problems. The design and implementation of this system is briefly reviewed. The final part of this chapter presents and discusses the results of validation tests using libtissue. A number of datasets containing system call and signal information were generated and a simple algorithm was implemented to test the libtissue sys-
tem. The behaviour of the algorithm is analysed and it is shown how the libtissue system can be used to build immune-inspired algorithms that detect anomalies in process behaviour.

**BIOLOGICALLY-INSPIRED APPROACHES**

Biological approaches to computer security are appealing for a number of reasons. Williamson (2002) discusses some of these reasons and their impact on the design of computer security systems. Biological organisms have developed many novel, parsimonious, and effective protection mechanisms. As computer systems and networks become more complex traditional approaches are often ineffective and suffer from problems such as scalability, and biologically systems are important sources of inspiration when designing new approaches. The short position paper of Morel (2002) discusses the general design of cyber-security systems that provides a large distributed computer network with a high degree of survivability. He proposes that a cyber-security system emulates the architecture of the biological immune system. As in this chapter, the innate immune system is considered as central to the immune response, processing information and controlling the adaptive immune system. An effective cyber-security system should emulate key features, most importantly distributed control, of the biological system, it should provide multiple information gathering mechanisms, and it should coevolve with the threat.

In another interesting position paper, Williams (1996) explores the similarities between people’s health and the security of complex computer systems. Humans are composed of distinct but tightly integrated multilayer systems, have external interfaces which can receive a wide range of input, and which carefully balance security and functionality, and have internal interfaces with protection mechanisms. They are not born with many of their defenses, but learn to protect themselves against recurring threats such as viruses, and are able to identify and develop defenses for new threats. The body is able to detect conditions that are likely to lead to injury. It is surrounded by a skin which, if damaged, leads to further response. Williams suggests that computer systems also need to have virtual skins with a similar functionality. He highlights the importance of the balance between functionality, security, and flexibility. Humans, as with computer systems, live a complex environment where conditions change over time. Both computer and biological systems are very sensitive to the input they receive. Biological systems check and filter input at many levels, and he suggests security systems need to do the same. He also emphasises the impossibility of accurate measurement of health in humans, which is reflected in the difficulty of measuring the security of computer systems. His general view is that the computer security industry is becoming as specialised as the healthcare industry, with security engineers akin to doctors.

Our interest is in immune-inspired approaches to intrusion detection. The field of artificial immune systems began in the early 1990s with a number of independent groups conducting research which used the biological immune system as inspiration for solutions to problems in other domains. There are several general reviews of artificial immune system research (Dasgupta, 2006; Hart & Timmis, 2005), and a number of books including Dasgupta (1999) and de Castro and Timmis (2002) covering the field. Large bibliographies have been collated by Dasgupta and Azeem (2006) (over 600 journal and conference papers), and an annual international conference has been held since 2002 (Proceedings of the International Conference on Artificial Immune Systems, http://www.artificial-immune-systems.org/). Specifically of relevance to this chapter is the review of artificial immune system approaches to intrusion detection by Aickelin, Greensmith, and Twycross (2004).

Intrusion detection systems are software systems designed to identify and prevent the misuse of computer networks and systems. Still a relatively young field, first discussed by James Anderson in his seminal 1980 paper (Anderson, 1980), and with the first working system described in Dorothy Denning’s 1987 paper (Denning, 1987), intrusion detection still faces many unresolved research issues. Many intrusion detection systems have been developed, representative samples of which are reviewed in Kemmerer and Vigna (2002) and Venter and Eloff (2003). Several excellent review papers (Axelsson, 2000; Bace & Mell, 2001) and books (Northcutt & Novak, 2003) on intrusion detection approaches have also been published. There are a number of different ways to classify intrusion detection systems (Axelsson, 2000). In their paper, Jansen and Karygiannis (1999) discuss the shortcomings of current intrusion detection system technology and the advantages of and approaches to applying mobile agents to intrusion detection and response. They
Related Content

An Integrated Security Verification and Security Solution Design Trade-Off Analysis Approach
[www.igi-global.com/chapter/integrated-security-verification-security-solution/23219?camid=4v1a](www.igi-global.com/chapter/integrated-security-verification-security-solution/23219?camid=4v1a)

Ontology-Based Authorization Model for XML Data in Distributed Systems
[www.igi-global.com/chapter/ontology-based-authorization-model-xml/40586?camid=4v1a](www.igi-global.com/chapter/ontology-based-authorization-model-xml/40586?camid=4v1a)

On Situational Aware En-Route Filtering against Injected False Data in Cyber Physical Systems
[www.igi-global.com/chapter/situational-aware-route-filtering-against/62386?camid=4v1a](www.igi-global.com/chapter/situational-aware-route-filtering-against/62386?camid=4v1a)

A Secure Hybrid Network Solution to Enhance the Resilience of the UK Government National Critical Infrastructure TETRA Deployment
[www.igi-global.com/article/secure-hybrid-network-solution-enhance/53012?camid=4v1a](www.igi-global.com/article/secure-hybrid-network-solution-enhance/53012?camid=4v1a)