Lancaster University
MANAGEMENT SCHOOL

Department of
Management Science
Seminar Series

Danger! Computer Security meets Operational Research

Dr Uwe Aickelin, Julie Greensmith
University of Nottingham – School of Computer Science & IT

Date: Thursday, February 15th, 2007
Time: 1 pm
Room: Lecture Theatre 6

Abstract: Artificial Immune Systems (AIS) are a collection of algorithms inspired by aspects of the human immune system. The arguably most obvious application of AIS was to detect intrusions in computer networks. If we can fight viruses with our immune systems, then surely we can fight computer viruses with a computer immune system? Early AIS approaches used a technique called Negative Selection, which did not provide a sufficient level of protection against intrusions. Problems were found with scalability and large numbers of false positives (false alarms) were generated. In 2003, Dr Uwe Aickelin and his colleagues proposed that the reason for the poor performance of the AIS is that Negative Selection is based on outdated concepts in immunology. It was proposed that the incorporation of the Danger Theory, a modern principle of immunology, could improve the performance of AIS when applied to intrusion detection. The result of the proposal is the Danger Project (EPSRC Adventure Fund) – an interdisciplinary collaboration between computer security experts, computer scientists, and 'wet-lab' immunologists. Recently, Uwe has been awarded an Advanced ESPRC Fellowship to investigate how OR models such as set covering problems can help direct future research. The work performed to achieve these goals is the focus of this part of the seminar.

Instead of trying to improve on existing heuristics, Julie Greensmith spent one year trying to understand the intricate methods the human immune system uses to detect invaders when the body is under attack. A novel idea in immunology is that the immune system releases danger signals in response to damage caused by infection. One cell in particular is involved in the collection and processing of danger signals. These cells are called Dendritic Cells (DCs). DCs are a major control unit cell of the human immune system, but were previously ignored by the AIS

community. In this seminar she will describe the process by which the behaviour of DCs is characterised and abstracted to form an algorithm – the Dendritic Cell Algorithm (DCA). The DCA is a population based algorithm, with each 'cell' acting as a signal processor and a data correlator. Julie will discuss the application of the DCA to the detection of a port scan. The results indicate an interesting future for this heuristic.

For further information please see www.dangertheory.com or www.aickelin.com

Bio: Uwe Aickelin is a Reader / Advanced EPSRC Research Fellow and Julie Greensmith a Research Associate in the School of Computer Science & IT at the University of Nottingham. Their research interests are mathematical modelling, heuristic optimisation, artificial immune systems and innate immunology applied to computer security problems.