

DANGER THEORY: THE MISSING LINK BETWEEN ARTIFICIAL IMMUNE SYSTEMS AND INTRUSION DETECTION

Creating a next generation Intrusion Detection System based on the latest Immunological Theories.

AISB Quarterly, Issue 115, pp 1-2, 2004.

The central challenge with computer security is determining the difference between normal and potentially harmful activity. For half a century, developers have protected their systems by coding rules that identify and block specific events. However, the nature of current and future threats in conjunction with ever larger IT systems urgently requires the development of automated and adaptive defensive tools.

A promising solution is emerging in the form of Artificial Immune Systems (AIS): The Human Immune System (HIS) can detect and defend against harmful and previously unseen invaders, so can we not build a similar Intrusion Detection System (IDS) for our computers? Presumably, those systems would then have the same beneficial properties as HIS like error tolerance, adaptation and self-monitoring.

Current AIS have been successful on test systems, but the algorithms were unable to scale up to real-world requirements. This is caused by their reliability on self-nonsel discrimination, as stipulated in classical immunology. However, immunologists are increasingly finding fault with traditional self-nonsel thinking and a new 'Danger Theory' (DT) is emerging.

This new theory suggests that the immune system reacts to threats based on the correlation of various (danger) signals and it provides a method of 'grounding' the immune response, i.e. linking it directly to the attacker. Little is currently understood of the precise nature and correlation of these signals and the theory is a topic of hot debate. It is the aim of this research to investigate this correlation and to translate the DT into the realms of computer security, thereby creating AIS that are no longer limited by self-nonsel discrimination. It should be noted that we do not intend to defend this controversial theory per se, although as a deliverable this project will add to the body of knowledge in this area. Rather we are interested in its merits for scaling up AIS applications by overcoming self-nonsel discrimination problems.

With our growing understanding of cellular components involved with apoptosis, it will be possible to compare the differential proteomic profile between necrotic ('bad') and apoptotic ('good' or 'planned') cell death, particularly with respect to Antigen Presenting Cells (APCs) activation. A vital necessity will be in maintaining the physiological relevance of the system to be utilised, so that the power of the DT in protecting against false positives will be preserved.

In essence, it is thought that apoptosis has a suppressive effect and necrosis a stimulatory immunological effect, although they might not actually be as distinct as currently thought. In the IDS context, this can be read in two ways: either the necrotic signals act to say that the previous pattern of apoptotic signals is dangerous or the apoptotic signals indicate that the necrotic signals are a false alarm.

A variety of contextual clues may be essential for a meaningful 'danger signal', and immunological studies will provide a framework of ideas as to how 'danger' is assessed in the HIS. Such ideas can be fruitfully applied to the AIS arena. In the latter context, the danger signals should show up after limited attack to minimise damage and therefore have to be quickly and automatically measurable. Once the danger signal has been transmitted, the AIS can react to those artificial antigens that are 'near' the emitter of the danger signal. This allows the AIS to pay special attention to dangerous components and would have the advantage of detecting rapidly spreading viruses or scanning intrusions at an early stage preventing serious damage. See Figure 1 for a graphical illustration.

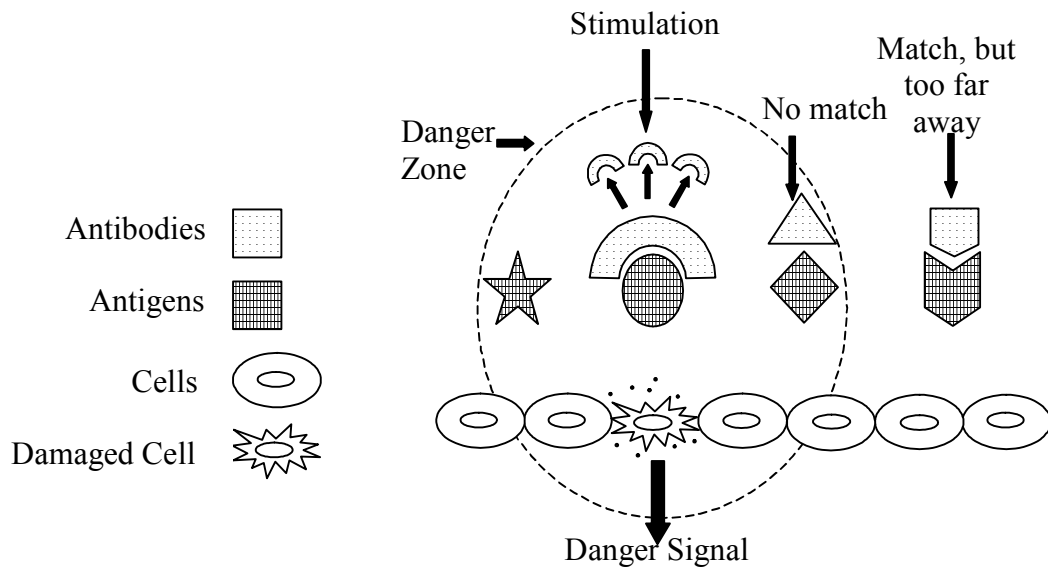


Figure 1: The Danger Theory Model.

This 3 year £657k project will start 1 January 2004 and is funded by the UK's Engineering and Physical Sciences Research Council, with further support from Hewlett Packard Labs Bristol and ECSC Computer Security Bradford. For more information please contact the Principal Investigator:

Dr Uwe Aickelin
 School of Computer Science
 University of Nottingham
uxa@cs.nott.ac.uk
<http://www.aickelin.com>