ON APPLYING TUNABLE ACTIVATION THRESHOLD (TAT) HYPOTHESIS TO NETWORK INTRUSIONS AND SPAM DETECTION

M. J. Antunes†1, L. A. Santos1, M. E. Correia1

1*Faculty of Sciences, University of Porto*
Center for Research in Advanced Computing Systems (CRACS)
Portugal

† E-mail: *mantunes@dcc.fc.up.pt*

The vertebrate Immune System (IS) has been one emergent and rich source of inspiration for new ideas on computer security and anomaly detection, like network intrusions and spam detection.

The IS challenges are two-fold and metaphorically speaking, they are similar to the major ones faced by a anomaly detectors. First, both has to implement and coordinate appropriate countermeasures against dangerous and evasive "non-self"entities. Secondly they have to guarantee that normal "self"body cells (corresponding to "normal"activity) are not harmed in the process.

Like spam filters, most commercially available network intrusion detection systems (NIDS) are knowledge-based systems that search for known attack signatures, being thus unable to cope with attack innovation. In another way, anomaly-based systems search for outliers of normal network activity. Despite conceptually they can be seen as a better alternative, the implementations currently available produces a high level of false alarms. In this poster we present an anomaly detection architecture based on the Tunable Activation Threshold (TAT) hypothesis as postulated by Grossman and Paul. We also present some preliminary results obtained with a TAT simulator developed by us.

The principles behind TAT imply that the current state of immune cells is reflected by their history of interactions with antigens, providing dynamic adjustments to cells' activation levels and responses. Network traffic and emails also have dynamic behaviour, as changes in either network usage or email subject are reflected in different (or new) data content. Our approach to anomaly detection and spam filtering makes use of TAT's T-Cell dynamic principles to modulate the application triggers, thus adapting to changes in "normal" content and new forms of "abnormal" data.