Clustering Insider Threat Behaviour: An Ultrametric Anomaly Detection System

Pedro Contreras*
Thinking Safe Ltd., Egham, England - pedro.contreras@acm.org

Fionn Murtagh
De Montfort University, Leicester, UK - fmurtagh@acm.org

Lee Hadlington
De Montfort University, Leicester, UK - lhadlington@dmu.ac.uk

Keith Scott
De Montfort University, Leicester, UK - jklscott@dmu.ac.uk

Anger, aggression and confrontational behaviour is one of 12 psychosocial precursors linked to malicious insider threat activity. Although there is not a given threshold at which these become a cause for concern, the manifestation of anger through aggressive language becomes relevant to indicate a potential insider threat, in particular when patterns of usage outside of normal behaviour are observed.

In previous work we have shown how an ultrametric can be used to create hierarchical clusters in constant algorithmic time, which is very well suited in the context of big data processing. In this work we introduce the use of such ultrametric applied to textual data in order to cluster anomalous aggressive behaviour. Our interest lies in detecting anomalies that can be used in conjunction with other behavioural precursors (e.g. stress, network traffic, etc.) to detect an insider threat. We complete our exposition demonstrating how this ultrametric can be used to obtain a raking of such behaviours.

Keywords: big data; ultrametric; clustering; insider threat.