The Prediction of Abnormal and Malicious Behavior: Automated Behavior Analysis (ABA)

Gary M. Jackson, PhD
Assistant Vice President and Technical lead
Science Applications International Corporation
6841 Benjamin Franklin Drive
Columbia, Maryland 21046
443-367-7716 Office
571-244-2225 Cell
gary.m.jackson@saic.com

The Prediction of Abnormal and Malicious Behavior: Automated Behavior Analysis (ABA)

This paper assumes that the identification and prediction of abnormal and malicious behavior is a function of an interaction between methodology and tools. The author has lead the development of patented methodologies and tools to identify threat, attacks, and first time cyber misuse. Using the psychology field of applied behavior analysis, automated behavior analysis (ABA) has surfaced as a set of behavioral science methodologies and automated tools to accurately predict adversarial behavior across a variety of domains. ABA is the only automation and extension of applied behavior analysis.

The field of applied behavior analysis stresses that behavior does not occur in a vacuum. Rather, behavior is only one component of a three-part sequence. This sequence is in the form of antecedents (A), behavior (B), and consequences (C) with components defined in the following manner:

Antecedent: Any event or situation occurring before the occurrence of the behavior that is logically related to the behavior.
Behavior: the actual definable and observable occurrence of the behavior of interest
Consequence: Any event or situation immediately following the occurrence of the behavior that is logically related to the behavior.

The basic premise of applied behavior analysis is that if antecedents and consequences associated with repeated occurrences of behavior can be identified, then the occurrence of that behavior in the future may be anticipated when the same or highly similar constellations of antecedent and likely consequence are present. The author has invented, refined, extended, and automated this model over the past three decades to be specifically relevant for anticipation of asymmetric threat. Validated across a wide variety of threat conditions, the SAIC patented model, methodologies, and applications have demonstrated real-time prediction with unprecedented accuracy, as well as the ability to identify key patterns existing between precursor antecedents and subsequent behavior to determine harmful intent of the individual being observed.

Tools for Identifying and Predicting Malicious Intent/Behavior
ABA as a set of methodologies consists of specific tools for constructing predictive models that may be embedded in specific adversarial threat applications. The following tools and applications have been used to predict terrorism, identify malicious intent from sensor based tracking, and determine malicious intent from network packets and are listed as representative ABA applications.

ThemeMate
A statistically based application that "reads" text descriptions of past examples of adversarial behavior and identifies/extracts predictors of behaviors of interest. Once predictive antecedents have been automatically identified, the application presents the user key conditions suitable for advanced prediction and influence. The application has been validated to produce major themes and summarize text in English and in Arabic. Multiple documents may be combined to provide

overall themes across examples of adversary behaviors, documents can be processed across time to provide shifts and trends, and single documents may be compared to determine similarities and differences. As a final product, the ThemeMate application produces a data array of all extracted antecedents by behavior example. This data array is then presented to AutoAnalyzer for automated pattern classification.

AutoAnalyzer

The AutoAnalyzer application offers the first automated approach to applied behavior analysis modeling. By presenting the data array produced by ThemeMate to AutoAnalyzer, the application automatically constructs a best practices pattern classifier, optimizes the pattern classifiersfor maximum predictive performance, validates the pattern classifier by testing against blind examples, produces overall validation accuracy, repeats the pattern classification process by constructing and validating additional classifiers with different configurations, and presents the highest accuracy model for real-time predictive use. By entering the presence or absence of the extracted antecedents for a given time to the trained classifier, the result is an immediate prediction or classification.

CheckMate and InMate

In addition to ThemeMate and AutoAnalyzer, the ABA technology has been embedded in two cyber applications. These tools are the *Checkmate Intrusion Protection System*, or *Checkmate*, and the *InMate Insider Threat Misuse System.* Both products represent new proactive and predictive technology to identify malicious cyber behavior not previously detected by signature detection or anomaly detection. Instead, the ABA applications represent real-time human behavioral assessment engines that make determinations of threat vs. no threat every $1/10^{th}$ of a second on an ongoing basis. Independent validation has demonstrated the capability to predict and identify new attacks and malicious intent.