

Security Modeling and Simulation to Address the Outsider Threat*

Use of Machine Learning Algorithms to Determine Features for Analysis

Dean Dominguez

International Security Engineering

Sandia National Laboratories

P.O. Box 5800, MS-0757, Albuquerque, New Mexico 87185-0757

ddoming@sandia.gov

ABSTRACT

Security modeling of adversary attacks has been an evolving science over the years. Sandia National Laboratories (SNL) is applying the Scenario Toolkit And Generation Environment (STAGE) commercial modeling and simulation software to develop scenarios for a demonstration facility that is being used by SNL for a variety of security training activities. To extend the range of simulation capabilities, machine learning algorithms are being utilized to perform a sensitivity analysis for future evaluations. These classification algorithms are being run utilizing current known simulation results, and determining the effect of each parameter modeled on the final result.

In a traditional simulation, a “force-on-force” approach is taken to model two opposing teams – an attacking force with malicious intent, and a defending force responsible for protection of a facility. Once a baseline configuration is established for each force representing their respective capabilities, an analyst is then able to perform “what-if” analysis by systematically modifying variables of interest. These variables could include additional adversaries/defenders, changes in weaponry, inclusion of technology (more cameras, or sensors), etc. Essentially, following the credo of “Gates, Guards, and Guns.” While historically, variations of Modeling and Simulation (map exercise, computer exercise, and ground exercise) are intended to be cost effective alternatives for a facility’s operating budget, there still continues to be a need for studying the whole breadth of problems within budget.

During the planning phase, the value of subject matter experts (SME) is extremely valuable in the field. Experts help determine the scope of the analysis, and what will likely be contributing criteria to a final analysis result. Otherwise, an analyst could spend years studying potential problems to the power of N. This is comparable to a “trouble shooting” phase where an analyst will try different combinations to determine what works. This paper will outline the results of applying machine learning algorithms to a known dataset that will determine which scenario parameters are more influential than others.

* Sandia National Laboratories is a multi program laboratory operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Company, for the U.S. Department of Energy’s National Nuclear Security Administration under Contract DE-AC04-94AL85000. SAND2012-XXXXC, approved for Unclassified/Unlimited Release.