A flexible Fuzzy Threat Evaluation Computer System

Essam M. Hamed' and Tarek **S.** Sobh'
1 Egyptian Armed Forces, Egypt

Abstract

This paper proposes a new approach for threat evaluation in distributed computing systems. Although anomaly-based threat detection systems are very helpful in detecting unknown attacks that are not defined in the signature and rule-based analysis of the misuse threat detection approach, there are many difficulties in accurately and efficiently performing anomaly threat detection. Tuning statistical anomaly threat detection engines is a significant challenge that often causes high false alarm rates. Also, many types of threats cannot be crisply defined and the degree of alert (threat level) that can occur with threats is often imprecisely defined.

The use of fuzzy logic in this paper is explored as a threat evaluation engine for an anomaly-based threat detection system by presenting a novel anomaly threat detection architecture using fuzzy logic to overcome the anomaly detection systems drawbacks and to present an accurate and flexible threat evaluation system.

Keywords: Anomaly threat detection, Threshold level, Statistical models, Historical profiles, Fuzzy logic, fuzzy membership function, Fuzzification, Degree of membership, and Threat evaluation.