A Cooperative Intrusion Detection Model Based on Granular Computing and Agent Technologies

Wei Zhang, School of Computers, Guangdong University of Technology, Guangzhou, China

Shaohua Teng, School of Computers, Guangdong University of Technology, Guangzhou, China

Haibin Zhu, Collaborative Systems Laboratory, Nipissing University, North Bay, Canada

Dongning Liu, School of Computers, Guangdong University of Technology, Guangzhou, China

ABSTRACT

This paper initially analyzes the methods of four attack types, including Probing, DoS (Denial of Service), R2L (Remote to Local) and U2R (User to Root). It then categorizes attacks into four cases which are, respectively, one host-one host, one host-many hosts, many hosts-one host and many hosts-many hosts. Categorization is based on resource and destination addresses of network packages. Granular computing methodology is then applied to intrusion detection. With the support of the granular computing methodology and agent technologies, a cooperative intrusion detection model is proposed. Furthermore, the construction for an intrusion detection agent is presented. Finally, experiments are conducted. Results indicate that the proposed method can detect slow scanning attacks which cannot be detected by a traditional scanning detector.

Keywords: *Agent, Attack, Cooperative Computing, DoS (Denial of Service), Granular Computing, Intrusion Detection, R2L (Remote to Local), U2R (User to Root)*

1. INTRODUCTION

In recent years, many scholars have conducted much research into the fundamental theories and application methods of granular computing. However, there are still few precise definitions for granular computing (Yao, 2008) . We can only find a conceptual description, that is, granular computing is a multi-disciplinary subject combining logical thinking, problem solving, and information processing methodology with their related theories and techniques (Yao, 2008)

DOI: 10.4018/ijats.2013070104

based on a multi-level granular structure. The research of granular computing relates itself with rough sets, fuzzy sets and the Dempster-Shafer theory, cluster analysis, decision trees, databases, machine learning, data mining, and many other fields.

Granular computing consists of particles, particle layers and grain structures (Wang et al., 2007). Particles are the basic elements of a granular computing model. A particle layer is the set of all the particles following the granulation guidelines of an actual demand, which is an abstract description of the problem space. A graining rule corresponds to a particle layer, and different granulating rules correspond to different particle layers. A rule reflects that people understand and observe the problem from different perspectives. Linkages among all grain layers constitute a relational structure, known as a grain structure (Wang et al., 2007). Graining refers to the decomposition of the problem space into multiple sub-spaces by gathering individuals in the problem space into different classes (grains), based on relevant information and knowledge. A granule is regarded as an instance of a corresponding concept. Granular computing includes: 1) problem solving taking particles as operands, 2) transformation on the same layer; and 3) mutual conversion and reasoning among different grain layers (Wang et al., 2007).

Network data structure has become increasingly complex due to the extensive application of networks and corresponding increases in data volume. Network security has become one of the most serious problems in the world. And there are many instances supporting this fact (Anonymous et al., 2003; Teng, 2008). Intrusion detection is one of the major technologies ensuring network security without affecting computer systems and network performance. It is a process that includes three steps: 1) collecting significant information from a number of key points in a computer system (network packets, host computer system log, the router information, etc.); 2) analyzing the information to detect intrusions; and 3) identifying the behavior of intrusions, the ongoing invasion or even intrusions that have happened before. Employing a single detection method or an agent makes it difficult to gather comprehensive data about intrusions and detect all intrusions. Reasons for such a difficulty are as follows: (1) networks have multiple entries and exits; (2) intrusion methods and means are versatile; (3) network complexity means that attacks are variable; and (4) attacks are deliberately disguised to escape detection.

In recent years, attackers have shown increasing sophistication in their ability to launch attacks that target or utilize a large number of hosts spread over a wide geographical area or multi-administrative-domains (Teng, 2008; CERT Coordination Center (CERT/CC), 2003). For example, attacks can scan large numbers of hosts simultaneously to search for software vulnerabilities; they can use self-replicating computer programs to spread their malicious codes to thousands of vulnerable systems within a short time; and they can use thousands of compromised hosts from different network domains to overload a targeted link or a system to disrupt its service. Such a disruption is called a DDoS (Distributed Denial-of-Service).

In order to detect these attacks, it is necessary to combine evidence of suspicious activity from multiple, geographically distributed networks. Rather than considering each Intrusion Detection System (IDS) in isolation, a Collaborative Intrusion Detection System (CIDS) (Teng, 2008) can be formed to analyze evidence from multiple networks simultaneously. By combing evidence from multiple networks, more attacks can be detected.

For these reasons, a cooperative intrusion detection method based on granular computing and agent technologies is proposed in this paper. A GrCoIDM (Granular-Computing-Cooperative-Intrusion-Detection-Model) is implemented.

The remainder of this paper is organized as follows. First, we review existing research. We then describe and analyze individual and coordinated attacks that have been observed on the Internet in the section afterwards. Followed by a section that classifies attacks into

Distributed Agency

Eugenio Dante Suarez and Manuel Castañón-Puga (2013). *International Journal of Agent Technologies and Systems (pp. 32-52).*
www.igi-global.com/article/distributed-agency/77664?camid=4v1a