Chapter 9
Generalized Evidential Processing in Multiple Simultaneous Threat Detection in UNIX

Zafar Sultan
University of New England, Australia

Paul Kwan
University of New England, Australia

ABSTRACT

In this paper, a hybrid identity fusion model at decision level is proposed for Simultaneous Threat Detection Systems. The hybrid model is comprised of mathematical and statistical data fusion engines; Dempster Shafer, Extended Dempster and Generalized Evidential Processing (GEP). Simultaneous Threat Detection Systems improve threat detection rate by 39%. In terms of efficiency and performance, the comparison of 3 inference engines of the Simultaneous Threat Detection Systems showed that GEP is the better data fusion model. GEP increased precision of threat detection from 56% to 95%. Furthermore, set cover packing was used as a middle tier data fusion tool to discover the reduced size groups of threat data. Set cover provided significant improvement and reduced threat population from 2272 to 295, which helped in minimizing the processing complexity of evidential processing cost and time in determining the combined probability mass of proposed Multiple Simultaneous Threat Detection System. This technique is particularly relevant to on-line and Internet dependent applications including portals.

1. INTRODUCTION

Computer security has become very critical issue in the IT industry. Almost every organization is facing security threats both from employees and outside intruders. Internet and Web and web portal IT systems are highly vulnerable to hackers and on many occasions, hackers have broken the existing security measures and have stolen million dollar information and damaged the IT infrastructure. The increasing complexity of the web portals

DOI: 10.4018/978-1-4666-0336-3.ch009

and internet architecture has simply widened and opened another area of security challenges for the whole IT industry. In order to protect organizations securities in terms of critical business and personal data, IT industry has to keep on strengthening their efforts to develop intrusion detection system. As a result, organizations need to spent billion of dollar just for securing and smooth run of their business data over the internet. For example Microsoft spent $1.2 billion to stop Sapphire/Slammer worm in 2003 (Ma, 2001; Spafford, 1991).

Business dependence on Internet-based services, and Internet-facing platforms such as enterprise portals, significantly increase the prospect of concerted security attacks. In spite of all these security measures and highly recommended Intrusion Detection Systems, hackers still continuously breaking companies securities, exploiting system weaknesses and perform illegal functions such as stealing important information, business secrets, damaging data or systems etc. etc. The biggest challenges in the security fields are the types of attack, their point of origin and the quantity of damage and of course to identify attack and block it in time is the most demanding aspect for the IT industry (Braun, 2000; Siaterlis & Maglaris, 2004).

Due to complexity of the UNIX applications infrastructure and Network architecture and implementation of multiple monitoring systems, false alarms have really become a big headache for the large companies. Millions of dollars have been spent just to build monitoring infrastructure but there does not seem to be any solution to stop false positive and false negatives. In general most of the Intrusion Detection Systems check the application layer, data layer and network layer data based on pattern matching with the existing situations of the processes and systems attributes. However, it is quite difficult to track an attacker if he / she just penetrate security and then keep steeling business data for months and months until new security updates find this attack but it is then too late. Damage has already been done. Looking into these facts, it looks a continuous battle between security implementers and hackers. But this is well known fact that an advancement of Intrusion Detection Systems have certainly reduced the number of security violation incidents and it has become more difficult for hackers to penetrate any IT systems that is well protected and secured using advance implementations of firewalls, intrusion detection system and monitoring systems (Bendjebbour et al., 2001; Hall, 1992).

The emphasis of our research is the experimental evaluation of the simultaneous multiple threat detection system using Multi-sensor data fusion, its various approaches and techniques in UNIX environments. Our research will help in building multiple simultaneous threat detection system for computer security in general and for web based applications, web portals and internet applications of UNIX environments in particular. The main target of this paper is an advance step to use Dempster Shafer, Weighted Dempster Shafer and Generalized Evidential Processing (GEP) theory for Multi-sensor data fusion whilst in our previous research experiment, We used only Dempster Shafer and weighted Dempster Shafer for data fusion. Therefore, in this paper we will provide numerical comparisons between Dempster Shafer, Weighted Dempster Shafer and Generalized Evidential Processing and compare their efficiency and performance.

2. EXISTING THREAT DETECTION APPROACHES IN UNIX

Parametric / non parametric techniques like Bayesian, Dempster Shafer, fuzzy rule and Kalman Filter are the most predominated techniques used for multiple threat detection in UNIX (Braun, 2000; Grocholsky, Makarenko, & Durrant-Whyte, 2003; Wu, Siegel, Stiefelhagen, & Yang, 2002). Theory of Set Cover, Chapman-Kalmogorov prediction model and method of least squares have also been used as an integral model with Bayesian,