Wild-Inspired Intrusion Detection System Framework for High Speed Networks

(φ|π) IDS Framework

Hassen Sallay, Imam Muhamad Ibn Saud Islamic University, Saudi Arabia
Mohsen Rouached, Imam Muhamad Ibn Saud Islamic University, Saudi Arabia
Adel Ammar, Imam Muhamad Ibn Saud Islamic University, Saudi Arabia
Ouissem Ben Fredj, Imam Muhamad Ibn Saud Islamic University, Saudi Arabia
Khalid Al-Shalfan, Imam Muhamad Ibn Saud Islamic University, Saudi Arabia
Majdi Ben Saad, Imam Muhamad Ibn Saud Islamic University, Saudi Arabia

ABSTRACT

While the rise of the Internet and the high speed networks made information easier to acquire, faster to exchange and more flexible to share, it also made the cybernetic attacks and crimes easier to perform, more accurate to hit the target victim and more flexible to conceal the crime evidences. Although people are in an unsafe digital environment, they often feel safe. Being aware of this fact and this fiction, the authors draw in this paper a security framework aiming to build real-time security solutions in the very narrow context of high speed networks. This framework is called (φ|π) since it is inspired by the elephant self-defense behavior which yields π (22 security tasks for 7 security targets).

Keywords: Cybernetic Attacks, Framework, High Speed Network, Intrusion Detection, Monitoring

INTRODUCTION

Our digital environment has a fact and a fiction. The fact is that virtual mice, snakes, bats, camels, foxes and wolves are there. Mice have no aim except the corruption, snakes spout venom everywhere, bats love to work in the dark, hateful camels look for revenge, foxes and wolf use cunning and Rogan to hit victims and conceal the crime. The fiction is that we often feel safe. Some behave as a peacock, proud of its security arsenal and infrastructure even if the attacks rain cats and dogs. Some others behave as an ostrich, only burying the head in the sand. Some others behave as a spider, pro-
tecting themselves by a security infrastructure as weak as a spider web. Being aware of this fact and this fiction, several efforts have been conducted in the literature. We survey briefly in the following some of these efforts from both industrial and academic sides.

From the industrial side, several real security platforms provide integral security solutions. They are known as hybrid IDS (Intrusion Detection System), since they are based on a merging between different techniques. We cite here CheckPoint IPS based mainly on Confidence indexing, Cisco IPS and BreachGate WebDefend based on behavior and statistical analysis, DeepNines BBX IPS, AirDefense Guard and BarbedWire IDS based on protocol analysis and data correlation (García-Teodoro et al., 2009). From academia, we cite the misuse based IDS Snort Inline and Snort with SPADE anomaly plug-in. Snort is largely considered as the de facto IDS (Roesch, 1999). BRO, from Lawrence Berkeley National Laboratory, is compatible with snort and includes semantic analysis at the application layer (Dreger et al., 2006), while EMERALD, from SRI laboratory, considers rule-based discovery and Bayesian networks (http://www.sdl.sri.com/projects/emerald/). Some others are based only on anomaly based techniques such that SPADE, Prelude, nPatrol and Mazu profiler (http://www.prelude-technologies.com/). Other research projects from the academic side yielded several interesting IDS frameworks and systems such as MINDS IDS from University of Minnesota (Ertoz et al, 2004), Orchids from ENS de Cachan (http://www.lsv.ens-cachan.fr/Software/orchids/), Intelligent IDS from Mississippi State University, GIDRE from University of Granada, Genetic Art- IDS from Northwestern University (García-Teodoro et al., 2009) and anagram form Columbia University. We note that the commercial systems basically tend to use well mature known techniques by enhancing their implementation issues while the research systems tend to use much more innovative techniques. Both sides use a large spectrum of techniques such as statistical methods, clustering techniques, diversification, Bayesian inference, genetic algorithms, payload modeling through n-grams, stochastic modeling, fuzzy logic, data mining and neural networks.

While the aforementioned systems provide interesting functionalities, they only partially satisfy the narrow constraints raised by the high speed network context, mainly the real-time criterion. Recently, new approaches and solutions addressing the huge amounts of transferred network data and increasing speeds of today’s networks were proposed. Guinde et al. (2010), Kang et al. (2006), Katashita et al. (2007), Kim et al. (2006), Clark et al. (2006), and Lin et al. (2006) aim to accelerate the speed of detection process by using specialized hardware mainly based on FPGA (Field-Programmable Gate Array) technology. Liberouter project (http://www.liberouter.org/projects.php) introduces the COMBO platform with the FlowMon probe and the IDS probe implemented by FPGA. Akhlaq et al. (2010) and Wenbao et al. (2006) proposed a solution based on traffic load balancing between different IDS sensors. In Akhlaq et al. (2010), the clustering technique was used. The load balancer distributes the traffic among cluster nodes on a predefined policy. The authors proposed a logic-ensured maximum utilization of cluster resources by exchanging state information, load sharing, reducing data loss and performing recovery evaluation procedure to maximize the overall efficiency. Wenbao et al. (2006) presented the design and implementation of a new approach for anomaly detection and classification over high speed networks. Mainly, the proposed approach is based on two phases. The first one is a data reduction phase through flow sampling by focusing mainly on short lived flows. The second step is then a random aggregation of some descriptors such as the number of SYN packets per flow in two different data structures. Salem et al. (2010), Foschini et al. (2008), Schuff et al. (2007), and Vallentin et al. (2007) consider the problem of real-time and scalable stateful intrusion detection for high-speed networks. Basically, the authors state that this problem cannot easily be solved by optimizing the packet matching algorithm utilized by a centralized process or
www.igi-global.com/chapter/automated-formal-methods-security-protocol/56300?camid=4v1a

Secure Agent Roaming for Mobile Business
www.igi-global.com/chapter/secure-agent-roaming-mobile-business/23262?camid=4v1a