A Host-Based Intrusion Detection System Using Architectural Features to Improve Sophisticated Denial-of-Service Attack Detections

Ran Tao, Louisiana State University, USA

Li Yang, University of Tennessee at Chattanooga, USA

Lu Peng, Louisiana State University, USA

Bin Li, Louisiana State University, USA

ABSTRACT

Application features like port numbers are used by Network-based Intrusion Detection Systems (NIDSs) to detect attacks coming from networks. System calls and the operating system related information are used by Host-based Intrusion Detection Systems (HIDSs) to detect intrusions toward a host. However, the relationship between hardware architecture events and Denial-of-Service (DoS) attacks has not been well revealed. When increasingly sophisticated intrusions emerge, some attacks are able to bypass both the application and the operating system level feature monitors. Therefore, a more effective solution is required to enhance existing HIDSs. In this article, the authors identify the following hardware architecture features: Instruction Count, Cache Miss, Bus Traffic and integrate them into a HIDS framework based on a modern statistical Gradient Boosting Trees model. Through the integration of application, operating system and architecture level features, the proposed HIDS demonstrates a significant improvement of the detection rate in terms of sophisticated DoS intrusions.

Keywords: *Architectural Features, Denial-of-Service (DoS) Attacks, Event Monitors, Host-Based IDS, Statistical Models*

INTRODUCTION

Denials of Service (DoS) attacks impose serious threat on the availability and quality of Internet services (Moore, Voelker, & Savage, 2001). They exhaust limited resources such as network bandwidth, DRAM space, CPU cycles, or specific protocol data structures, inducing service degradation or outage in computing infrastructures for the clients. System downtime

DOI: 10.4018/jisp.2010010102

resulting from DoS attacks could lead to million dollars' loss.

Generally, DoS attacks can be either flooding-based or software exploit-based. In a flooding-based DoS attack, a malicious user sends out a tremendously large number of packets aiming at overwhelming a victim host. For example, in a SYN-flooding attack, a significant number of TCP SYN packets are sent towards a victim machine, saturating resources in the victim machine. We can observe a surge of TCP connections in a short time, which are modeled by a tuple of application features <*source IP*, *destination IP*, *source port*, *destination port*>. In exploit-based DoS attacks, specially crafted packets are sent to the victim system targeting at specific software vulnerabilities in the operating system, service or application. The success of exploitation will either overwhelm or crash the target system. An existing solution to the exploit-based attacks is to patch and update software frequently.

Currently, research work on DoS intrusion detections mainly rely on Network-based Intrusion Detection Systems (NIDSs) (Chen et al., 2005; Handley et al., 2001; Hussain et al., 2003; Jin et al., 2003; Chari et al., 2003; Kuzmanovic et al., 2003; Wang et al. 2003). The NIDSs monitor features extracted from network packet headers at the application layer such as packet rate and traffic volume. Ramp-up behaviors and frequency domain characteristics are also studied to aid in improving the accuracy and performance of IDS (Chen et al., 2005; Hussain et al., 2003). On the other hand, Host-based Intrusion Detection Systems (HIDSs) which widely employ audit trails and system call tracking can effectively identify buffer overflow (BoF) attacks (Chari et al., 2003; Chaturvedi et al., 2006; Wagner et al., 2002). However, the DoS attacks are not easily observed by such an HIDS and not widely researched in the HIDS literature. Some researchers have proposed to limit the bound of certain system calls (Chari et al., 2003) such as fork(). However, with the advent of large-scale application software, such bounds may seriously impair the performance of normal applications. Moreover, DoS attacks may not involve huge number of system calls at all. Therefore, a more generic solution is needed to detect DoS attacks.

When increasingly sophisticated techniques are adopted by attackers, multi-tier attacks and IP spoofing are emerging to amplify destructive effects and evade detections. The attack patterns or behaviors will be difficult to identify by using only header-based network traffic analysis. For example, in a complicated scenario that an attacker gets around the network monitoring sensors and launches DoS attacks locally, a NIDS may not able to detect this intrusion. In such a scenario, non-privileged access is well enough to successfully initiate a DoS attack against the host machine: once the attacker obtains the access to the victim machine, even if it is not root-privileged and difficult to further elevate to carry out other destructive or stealthy behaviors, he/she can still easily upload a DoS daemon to massively consume the machine's limited resources. Instead of network information only, information originated and resided on the victim machine should be used to track and monitor such undergoing attacks in this case.

In this paper, we propose an HIDS with multi-level integrated information from application, operating system (OS), and architecture levels to improve the detection rate of sophisticated DoS attacks. According to our experiments, even if DoS attacks could successfully evade captures of NIDS monitors, architectural behaviors will still be triggered: a tremendous jump of *Instruction Count*, *Cache Miss*, *Bus Traffic* can be found. Based on this observation, a novel HIDS employing a modern statistical *Gradient Boosting Trees (GBT)* model is proposed to detect sophisticated DoS intrusions through the integration of application, OS, and architecture features. Our experiments test three different types of exploits: self-developed local DoS exploits, real-world remote DoS exploits and real-world local DoS attacks. The results show that the inclusion of architecture features can significantly improve the detection rate of evasive DoS intrusions.

Toward Proactive Mobile Tracking Management

Hella Kaffel Ben Ayed and Asma Hamed (2014). *International Journal of Information Security and Privacy (pp. 26-43).*
www.igi-global.com/article/toward-proactive-mobile-tracking-management/140671?camid=4v1a