Chapter 17
An Auto-Reclosing-Based Intrusion Detection Technique for Enterprise Networks

Nana K. Ampah
Jacobs Engineering Group, USA

Cajetan M. Akujuobi
Prairie View A&M University, USA

ABSTRACT

Designing, planning, and managing telecommunication, industrial control, and enterprise networks with special emphasis on effectiveness, efficiency, and reliability without considering security planning, management, and constraints have made them vulnerable. They have become more vulnerable due to their recent connectivity to open networks with the intention of establishing decentralized management and remote control. Existing Intrusion Prevention and Detection Systems (IPS and IDS) do not guarantee absolute security. The new IDS, which employs both signature-based and anomaly detection as its analysis strategies, will be able to detect both known and unknown attacks and further isolate them. Auto-reclosing techniques used on long rural power lines and multi-resolution techniques were used in developing this IDS, which will help update existing IPSs. It should effectively block Distributed Denial of Service attack (DDoS) based on SNY-flood attacks and help eliminate four out of the five major limitations of existing IDSs and IPSs.

INTRODUCTION

Enterprise networks are the main targets for hackers or intruders due to the fact that most financial transactions take place online and the networks also handle vast amounts of data and other resources (Satti & Garner, 2001). Handling transactions online is on the increase every day because it makes life easier for both the customers as well as the enterprises offering services (Jou et al., 2000; Yau & Xinyu Zhang, 1999; Ko, 2003; Tront & Marchany, 2004). Enterprise networks also have lots of bandwidth, which is very attractive to hackers because they take advantage of that by using those networks as launching pads to attack others (Tront & Marchany, 2004; Janakiraman,

DOI: 10.4018/978-1-4666-7381-6.ch017

Waldvogel, & Qi Zhang, 2003). It therefore becomes very difficult for the IDSs and IPSs at the receiving end to detect and prevent the attacks or hackers, since the packet header information will indicate legitimate senders. This is the main reason why most IPSs are easily bypassed by hackers (Tront & Marchany, 2004; Paulson, 2002; Weber, 1999). Intrusion prevention, which is a proactive technique, prevents the attacks from entering the network. Unfortunately, some of the attacks still bypass the intrusion prevention systems. Intrusion detection on the other hand, detects attacks only after they have entered the network.

Although attacks are generally assumed to emanate from outside a given network, the most dangerous attacks actually emanate from the network itself. Those are really difficult to detect since most users of the network are assumed to be trusted people. The situation has necessitated drastic research work in the area of network security, especially in the development of intrusion detection and prevention systems intended to detect and prevent all possible attacks on a given network (Akujuobi & Ampah, 2007; Akujuobi, Ampah, & Sadiku, 2007).These IDSs use either anomaly or signature-based detection techniques. Anomaly detection techniques detect both known and unknown attacks, but signature-based detection techniques detect only known attacks. The main approaches of anomaly detection techniques are statistical, predictive pattern generation, neural networks, and sequence matching and learning (Palnaty, & Rao, 2013; Suthaharan, 2012; Aljarah, & Ludwig, 2013; Strasburg, Basu, & Wong, 2013; Kumar, Hanumanthappa, & Kumar, 2012; Gupta, Pandey, Shukla, Dadhich, Mathur, & Ingle, 2013; Ganapathy, Kulothungan, Yogesh, & Kannan, 2012; Thaseen, & Kumar, 2013; Tomasek, Cajkovsky, & Mados, 2012; Quang Anh Tran, Jiang, & Jiankun Hu, 2012; Sadighian, Zargar, Fernandez, & Lemay, 2013). The main approaches of signature-based detection techniques are expert systems, keystroke monitoring, model-based, state transition analysis, and pattern matching (Mahdinia, Berenjkoob, & Vatankhah, 2013; Barhate, & Jaidhar, 2013; Mechtri, Tolba, & Ghanemi, 2012; Thaseen, & Kumar, 2013; Kumar, & Hanumanthappa, 2013; Biermann, Cloete, & Venter, 2001). There is no existing IDS or IPS that can detect or prevent all intrusions. For example, configuring a firewall to be 100% foolproof compromises the very service provided by the network. The use of conventional encryption algorithms and system level security techniques have helped to some extent, but not to the levels expected (Fadia, 2006; Leinwand & Conroy, 1996; Stallings, 2003). The following are the five limitations associated with existing IDSs (Satti & Garner, 2001):

1. **Use of Central Analyzer:** Whenever the central analyzer is attacked by an intruder the whole system will be without protection, so it becomes a single point of failure (Janakiraman, Waldvogel, & Qi Zhang, 2003);
2. **Limited Scalability:** Processing all data at a central point limits the size of the entire network that can be monitored and controlled at a time. Data collection in a distributed fashion also causes excessive traffic in the network (Kayacik, Zincir-Heywood, & Heywood, 2004);
3. **Effectiveness:** The ability of existing IDSs/ IPSs to detect and prevent intrusion is still not clearly established because of high false positive and false negative rates (Chunmei, Mingchu, Jianbo, & Jizhou, 2004);
4. **Efficiency:** Quantifying resources like time, power, bandwidth, and storage used by existing IDSs will be a critical success factor (Khoshgoftaar & Abushadi, 2004); and
5. **Security:** Securing the security data itself from intruders is also a very important limitation to existing IDSs.