Chapter I
Statistical Opportunities, Roles, and Challenges in Network Security

To me, a personal computer should be small, reliable, convenient to use and inexpensive.
- The Apple-II, Stephen Wozniak

INTRODUCTION

In this chapter, we will provide a brief overview of network security and introduce essential concepts of intrusion detection and prevention and review their basic principles and guidelines. Then, we will discuss statistical approaches in practice as well as statistical opportunities, roles, and challenges in network security.

Network security has become a very popular topic. A simple Google search based on the keyword “network security” showed 2.2 million items on February 29, 2008. Network security aims to protect the entire infrastructure of a computer network and its corresponding services from unauthorized access. The two key elements of network security are risk assessment and risk management. There are several fundamental components in network security: (1) security-specific infrastructures, such as hardware- and software-based firewalls and physical security approaches, (2) security polices, which include security protocols, users’ authentications, authorizations, access controls, information integrity and confidentiality, (3) detection of malicious programs, including anti-viruses, worms, or Trojan horses, and spyware or malware, and (4) intrusion detection and prevention, which encompasses network traffic surveillance and analyzing and profiling user behavior. Since the topic of network security links a great number of research areas and disciplines, we will focus on the component of intrusion detection and prevention in this book. Readers

The use of statistical techniques in network security for intrusion detection and prevention has attracted great attention by researchers from both statistical and computer science fields. The idea behind intrusion detection and prevention is to use normal (anomaly-free) patterns of legitimate user behavior to identify and distinguish the behavior patterns of anomalous users (Anderson, 1972; Anderson, 1980; Stallings, 2003), and although this idea seems simple, intrusion detection and prevention are difficult tasks to implement and each have their own set of unique challenges. This discipline is in development and many difficult topics for research need to be addressed (INFOSEC Research Council, 1999; McHugh, 2000b; Taylor & Alves-Foss, 2002). Ideally, a perfect detection system needs four essential characteristics: (1) the ability to detect a wide variety of intrusions, (2) the ability to detect intrusions in a timely fashion, (3) the ability to present the analysis in a simple format, and (4) the ability to perform these tasks accurately (Bishop, 2003). Although statistical methods have been adapted to achieve these goals over the past decades (Anderson, 1980; Vaccaro & Liepins, 1989; Lunt & Jagannathan, 1988; Smaha, 1988; Teng, Chen & Lu, 1990; Anderson, Frivold & Valdes, 1995; Forrest, Hofmeyr, Somayaji & Longstaff, 1996; Qu, Vetter & Jou, 1997; Neumann & Prras, 1999; Masum, Ye, Chen & Noh, 2000; Valdes & Skinner, 2000; Barbard, Wu & Jajodia, 2001; Jha, Tan & Maxion, 2001; Taylor & Alves-Foss, 2001; Zhang, Li, Manikopoulos, Jorgenson & Ucles, 2001; Ye, Emran, Chen & Vilbert, 2002; Shyu, Chen, Sarinnapakorn, & Chang, 2003; Zhou & Lang, 2003; Qin & Hwang, 2004; Leung & Leckie, 2005; Wang 2005; Wang & Cannady 2005, Wang & Seidman, 2006; Wang & Normand, 2006; Gharibian & Ghorbani, 2007; Khan, Awad & Thuraisingham, 2007; Wang 2007; Herrero, al. et., 2007; Nayyar & Ghorbani, 2008), the gap between the performance of what we expect and what is currently available in both intrusion detection and intrusion prevention systems is still remarkable. With rapid advancements being made in computer and network technology, as well as increasing information and national security threats, the demand for reducing this gap has increased significantly; regardless, there are great challenges and technical difficulties in overcoming such a gap. In the following sections, we will briefly review previous studies and discuss some basic challenges. More historical information and trends on this topic also can be found from McHugh (2000b) and Patcha & Park (2007).

**OVERVIEW**

Although the idea behind intrusion detection is simple—using normal patterns of legitimate user behavior to identify and distinguish the behavior of an anomalous user, intrusion detec-
Statistical Analysis Software
www.igi-global.com/chapter/statistical-analysis-software/29694?camid=4v1a