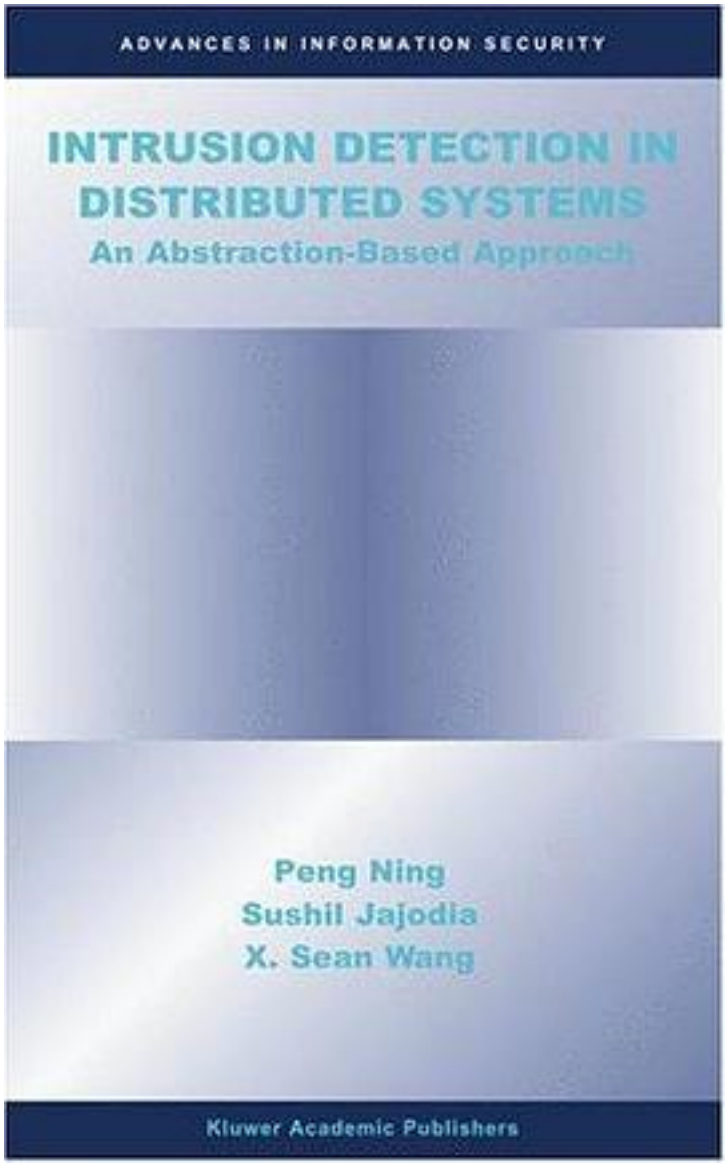
Intrusion Detection in Distributed Systems



Intrusion Detection in Distributed Systems_下载链接1_

著者:Peng Ning

出版者:Springer

出版时间:2003-10-31

装帧:Hardcover

isbn:9781402076244

Intrusion detection systems (IDS) are usually deployed along with other preventive security mechanisms, such as access control and authentication, as a second line of defense that protects information systems. Intrusion detection complements the protective mechanisms to improve the system security. Moreover, even if the preventive security mechanisms can protect information systems successfully, it is still desirable to know what intrusions have happened or are happening, so that the users can understand the security threats and risks and thus be better prepared for future attacks. Intrusion detection techniques are traditionally categorized into two classes: anomaly detection and misuse detection. Anomaly detection is based on the normal behavior of a subject (e.g., user or a system); any action that significantly deviates from the normal behavior is considered intrusive. Misuse detection catches intrusions in terms of characteristics of known attacks or system vulnerabilities; any action that conforms to the pattern of known attack or vulnerability is considered intrusive. Alternatively, IDS may be classified into host-based IDSs, distributed IDSs, and network based IDSs according to the source of the audit information used by each IDS. Host-based IDSs get audit data from host audit trails and usually aim at detecting attacks against a single host; distributed IDSs gather audit data from multiple hosts and possibly the network and connects the hosts, aiming at detecting attacks involving multiple hosts; network-based IDSs use network traffic as the audit data source, relieving the burden on the hosts that usually provide normal computing services. Intrusion Detection In Distributed Systems: An Abstraction-Based Approach presents research contributions in three areas with respect to intrusion detection in distributed systems. The first contribution is an abstraction-based approach to addressing heterogeneity and autonomy of distributed environments. The second contribution is a formal framework for modeling requests among cooperative IDSs and its application to Common Intrusion Detection Framework (CIDF). The third contribution is a novel approach to coordinating different IDSs for distributed event correlation. Intrusion Detection In Distributed Systems: An Abstraction-Based Approach is designed for a professional audience, composed of researchers and practitioners in industry. This book is also suitable as a secondary text for graduate-level students in computer science and electrical engineering.

作者介绍:

目录:

标签

评论

Intrusion Detection in Distributed Systems_下载链接1_

书评

Intrusion Detection in Distributed Systems_下载链接1_