Journal of Network and Computer Applications 57 (2015) 71–84

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

journal homepage: www.elsevier.com/locate/jnca

Review

Network defense: Approaches, methods and techniques

Rup Kumar Deka [a,*], Kausthav Pratim Kalita [a], D.K. Bhattacharya [a], Jugal K. Kalita [b]

[a] Department of Computer Science and Engineering, Tezpur University, Napaam, Assam, India
[b] Department of Computer Science, College of Engineering and Applied Science, University of Colorado, Colorado Springs, CO, United States

ARTICLE INFO

Article history:
Received 5 December 2014
Received in revised form
26 May 2015
Accepted 13 July 2015
Available online 26 July 2015

Keywords:
DoS
Intrusion
Defense
Response
Tolerance

ABSTRACT

To defend a network from intrusion is a generic problem of all time. It is important to develop a defense mechanism to secure the network from anomalous activities. This paper presents a comprehensive survey of methods and systems introduced by researchers in the past two decades to protect network resources from intrusion. A detailed pros and cons analysis of these methods and systems is also reported in this paper. Further, this paper also provides a list of issues and research challenges in this evolving field of research. We believe that this knowledge will help to create a defense system.

Contents

* Corresponding author.
E-mail addresses: rup.deka@gmail.com (R.K. Deka), koztov.project@gmail.com (K.P. Kalita), dkb@tezu.ernet.in (D.K. Bhattacharya), jkalita@uccs.edu (J.K. Kalita).

http://dx.doi.org/10.1016/j.jnca.2015.07.011
1084-8045/

1. Introduction

Computerization and internetization of the world is happening at an astonishing speed. In spite of growth at breakneck pace, service providers are doing their best to provide the highest quality of service. At every step, an aspect that stands out is security, which is indeed a very serious topic of concern. An intrusion or attack may be fast or slow. When an attack uses large size packets or extremely high volume traffic within a very short time, say a fraction of a minute, to disrupt service, it can be termed a fast attack. On the other hand, some attacks take minutes or hours to complete the process, and are referred to as slow attacks.

Frequently, network or system activities are carried out with malicious intentions or other network policy violations take place. This type of attempt or activity can be termed intrusion and its creator is known as an intruder. The goal of intrusion detection is to make the whole network secure by thwarting attempts to compromise confidentiality, integrity or availability of resources.

1.1. Motivation

There are several published surveys on approaches to intrusion detection and/or prevention such as Patel et al. (2010), Bhuyan et al. (2014b), Hoque et al. (2013), Kumar (2007), Richhariya and Srivastava (2013), and Patel et al. (2013). These authors usually provide details of a few approaches although some cover a larger number of defense systems. Bhuyan et al. (2014a) present a comprehensive survey of DDoS attacks, detection methods and tools used in wired networks. Hoque et al. (2013) provide a taxonomy of attack tools and also present a comprehensive and structured survey of existing tools and systems that can support both attackers and network defenders. An exhaustive survey of intrusion defense systems is presented by Patel et al. (2013), where the authors discuss approaches against intrusion by creating a layered taxonomy in addition to discussing cloud-based intrusion defense systems. Neither of the surveys by Patel et al. (2010) and Richhariya and Srivastava (2013) include issues of defense, challenges and solutions. In this paper we present a structured and comprehensive survey of defensive approaches, in terms of general overview, modules of a defense architecture, infrastructure and a taxonomy. We also attempt to present challenges in developing effective defensive approaches.

This paper provides a structured and comprehensive survey of approaches to counter intrusions. The major contributions of this survey are the following.

- Our presentation is more streamlined. First, we describe a defense system, in particular whether it detects or prevents intrusions considering the modules it contains. Then we focus on various detection techniques. Infrastructure needs, location and control of defense systems are also discussed.
- Most existing surveys do not fully cover the large number of issues, related to intrusion defense systems, but we do.
- We present a taxonomy to ensure that we cover a large area within the intrusion defense process.
- We also identify challenges encountered by approaches to prevent intrusions.

1.2. Prior surveys

Richhariya and Srivastava (2013) address issues of information security and describe the security needs of an organization to protect its critical information from attacks. A well-trained staff of analysts is required to continuously monitor the system. In such an environment, a huge amount of effort is required to construct new security strategies. Patel et al. (2010) review current trends in intrusion detection together with a study of implemented technologies. Kabiri and Ghorbani (2005) identify main categories of intrusion detection and prevention systems. They also provide a comparison of various approaches. Rathore (2012) also provides a survey of different approaches to intrusion detection. Sandhu et al. (2011) reviews methods for building intrusion detection and prevention systems (IDPSs) and uses a cost-effective intrusion detection and prevention method based on the concept of intelligent mobile agents to design an effective agent based intrusion prevention system (AIPS). AIPS works well in a distributed environment due to the use of software agents.

Murali (2005) surveys recent IDPSs and alarm management techniques by providing a comprehensive taxonomy and investigating possible solutions to detect and prevent intrusions in cloud computing systems. Considering the desired characteristics of IDPSs and cloud computing systems, a list of requirements is identified and four concepts of autonomic computing, viz., self-management, ontology, risk management, and fuzzy theory are leveraged to satisfy these requirements.

A survey of technologies for defense against intrusion is given in Patel et al. (2013). This paper discusses aspects of intrusion defense systems and data collection techniques. Data mining-based and data fusion-based IDSs are discussed to emphasize the need for large-scale data collection. Current defense technologies face powerful challenges and these are also described here, along with some suggested methods to overcome them.

Bai and Kobayashi (2003) describe detailed designs of both signature and anomaly-based NIDS (Network-based Intrusion Detection System).Requirements of such systems are thoroughly discussed. Kumar (2007) presents a nomenclature of IDSs that he uses for his survey. This paper also identifies strengths as well as the limitations of several IDSs (Table 1).

Our survey differs from these previous surveys in the following ways.

- In all the papers mentioned in this section, there is little information regarding where to deploy IDSs and other details of issues in deployment of IDSs.
- Most papers, which are mentioned in this section, do not provide any discussion of challenges faced when an intrusion defense system is deployed.
- We describe modules of an intrusion defense model in this paper. A thorough understanding of these modules is necessary to develop successful defense systems. Such discussions are not usually found in other survey papers.