Journal of Network and Computer Applications 62 (2016) 53–74

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

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

Review

Intrusion response systems: Foundations, design, and challenges

Zakira Inayat [a,b,*], Abdullah Gani [a,c], Nor Badrul Anuar [c,**], Muhammad Khurram Khan [d], Shahid Anwar [e]

[a] Center for Mobile Cloud Computing Research (C4MCCR), University of Malaya, 50603 Kuala Lumpur, Malaysia
[b] Department of Computer Science, University of Engineering and Technology Peshawar, Peshawar 2500, Pakistan
[c] Faculty of Computer Science and Information Technology, University of Malaya, 50603 Kuala Lumpur, Malaysia
[d] Center of Excellence in Information Assurance (CoEIA), King Saud University, Riyadh, Saudi Arabia
[e] Faculty of Computer System and Software Engineering, Universiti Malaysia Pahang, 26300 Gambang, Malaysia

ARTICLE INFO

Article history:
Received 21 September 2015
Received in revised form
17 December 2015
Accepted 23 December 2015
Available online 31 December 2015

Keywords:
Intrusion detection
Intrusion response
Semantic coherence
Response design parameter

ABSTRACT

In the last few decades, various network attacks have emerged. This phenomenon requires serious consideration to address its extensive consequences. To overcome the effects of network attacks, an appropriate intrusion detection system and a real-time intrusion response system are required. In this paper, we present an IRS taxonomy based on design parameters to classify existing schemes. Furthermore, we investigate the essential response design parameters for IRS to mitigate attacks in real time and obtain a robust output. The majority of existing schemes disregard the importance of semantic coherence and dynamic response parameters in the response selection process. Therefore, most existing schemes produce inaccurate results by generating false alarms. These design parameters are comprehensively discussed in this paper. We have qualitatively analyzed existing IRS schemes on the basis of the response design parameters. Open research challenges are identified to highlight key research areas in this research domain.

Contents

* Corresponding author.
** Principle corresponding author.
E-mail address: Zakirainayat@uetpeshawar.edu.pk (Z. Inayat).

http://dx.doi.org/10.1016/j.jnca.2015.12.006
1084-8045/

1. Introduction

For years, network security has been the focus of substantial research (Cisco, 2014). In the last few decades, humans have become increasingly technology-dependent (e.g., use of the Internet for business, educational, and social activities). A number of security incidents, including threats to confidentiality, integrity, and data availability, have occurred because of the excessive use of computer networks. The availability of computer networks and the integrity of data must be secure enough from intrusions, which include denial of service (DoS) attacks, unauthorized access, spoofing attacks, and application layer attacks (Hansman and Hunt, 2005; Hoque et al., 2014). Moreover, the annual report published by the Computer Emergency Response Team (CERT) indicates that the rate of intrusions is increasing every year (CERT, 2014). The Malaysian CERT in 2014 indicated a 50% increase in intrusions and reported more than 10,000 incidents (MyCert-Report, 2014). These reports prove that the effect of intrusions is unavoidable. Thus, a security mechanism is needed to enforce the security policies and overcome intrusions.

Security mechanisms, such as firewalls, authentication, cryptography, and access control are used as the first line of defense to security problems and issues (Kruegel et al., 2005; SANS Institute, 2003). However, these anti-threat applications are unable to detect internal intrusions and inadequately provide security countermeasures. Therefore, various types of intrusion systems that originated from intrusion detection systems (IDSs), such as intrusion prevention systems (IPSs) and intrusion response systems (IRSs), were developed to detect, prevent, and respond to intrusions (Anuar et al., 2010). An IDS is a collection of software or hardware resources that can detect, analyze, and report intrusions in a computing system. As an extension of IDS, an inline IDS or IPS detects and prevents potential intrusions in real time (Scarfone and Mell, 2007a). However, IPS requires high-performance systems and are difficult to manage in analyzing and preventing intrusions at the same time, particularly in a distributed environment. Thus, a security countermeasure that continuously monitors system performance is needed to effectively identify and handle potential incidents. This countermeasure is called IRS.

On the basis of the level of automation, IRSs are classified into notification, manual, and automated response systems (Stakhanova et al., 2007b). Despite the significant emphasis given to IDS and IPS, the detection of intrusions will be useless without an appropriate response system to thwart intrusions. To the best of our knowledge, three surveys (Shameli-Sendi et al., 2014, 2012; Stakhanova et al., 2007b) provide the classification of IRS and emphasize the important aspects related to IRS and its security issues. These surveys classified IRS into two categories, such as automated and non-automated, on the basis of their functionality. Furthermore, these surveys categorized IRS into cost-sensitive, adaptive, and non-adaptive IRS. In (Stakhanova et al., 2007b), the IRS design is based on the degree of automation, time of response, cooperation ability, and response selection method are described. In Shameli-Sendi et al. (2012), it is stated that the efficient response design is associated with the cost-sensitivity of the response and the prediction of minimum damage cost based on response cost. In Shameli-Sendi et al. (2014), the author proposed a taxonomy for intrusion risk assessment (IRA) and presented integrating risk assessment techniques. Consequently, existing surveys indicate that the effective coordination between intrusion response and risk assessment leads to an efficient framework to manage uncertainty in IRS.

Many studies have been conducted on IRS design and classification. However, existing IRS designs employ a static approach in selecting an optimum response option and lack semantics for intrusion alerts generated by the IDSs at distributed locations in the network (Mateos et al., 2012). Instead of choosing a flexible response metric, existing response systems (Mu and Li, 2010; Stakhanova et al., 2007a) use static response metrics, such as static risk threshold metric, severity metric, IDS confidence metric, and damage reduction metric. Consequently, the systems have difficulty in real time detection and response, false alarm management, and uncertainty in IRS (Anuar et al., 2008; Hubballi and Suryanarayanan, 2014). Therefore, there is a need for IDS and IRS to dynamically adapt, so as to detect and respond automatically. However, this paper proposes response design parameters for designing an efficient IRS, particularly in a distributed environment. The addition of these response design parameters in existing IRS design will result in an automated IRS with no false-alarm rates, low uncertainty, and proficiency to respond dynamically in real time. Thus, the contributions of this paper are as follows:

- A detailed literature survey that analyzes the latest trends in IDS and IRS and highlights the challenges that exist in the design of existing IRS.
- A taxonomy of the design attributes to enhance the design of IRS by proposing some essential response design metrics and identifying the main areas that need to be improved in IRS design.
- A comparative study based on the design metrics of IRS to prevent attacks, integrate new enhancements, and determine future research trends for experts and general users.

The rest of this paper is organized as follows. Section 2 discusses the selected studies and classifies the earlier stage of IDS.