Available online at www.sciencedirect.com

ScienceDirect

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

Computers & Security

Taxonomy of intrusion risk assessment and response system

Alireza Shameli-Sendi [a,*], Mohamed Cheriet [a], Abdelwahab Hamou-Lhadj [b]

[a] Department of Electrical and Computer Engineering, Ecole de Technologie Superieure (ETS), Montreal, Canada
[b] Department of Electrical and Computer Engineering, Concordia University, Montreal, Canada

ARTICLE INFO

Article history:
Received 14 December 2013
Received in revised form
30 March 2014
Accepted 27 April 2014
Available online 9 May 2014

Keywords:
Intrusion detection system
Intrusion response system
Intrusion risk assessment
Response time
Prediction
Response cost
Attack graph
Service dependency graph

ABSTRACT

In recent years, we have seen notable changes in the way attackers infiltrate computer systems compromising their functionality. Research in intrusion detection systems aims to reduce the impact of these attacks. In this paper, we present a taxonomy of Intrusion Response Systems (IRS) and Intrusion Risk Assessment (IRA), two important components of an intrusion detection solution. We achieve this by classifying a number of studies published during the last two decades. We discuss the key features of existing IRS and IRA. We show how characterizing security risks and choosing the right countermeasures are an important and challenging part of designing an IRS and an IRA. Poorly designed IRS and IRA may reduce network performance and wrongly disconnect users from a network. We propose techniques on how to address these challenges and highlight the need for a comprehensive defense mechanism approach. We believe that this taxonomy will open up interesting areas for future research in the growing field of intrusion risk assessment and response systems.

1. Introduction

Today's society relies increasingly on network services to manage its critical operations in a variety of domains including health, finances, public safety, telecommunication, and so on. It is therefore important to maintain high-availability and adequate response time of these services at all time. This is threatened by the presence of hostile attackers that look for ways to gain access to systems and infect computers (Zhou et al., 2010). To mitigate these threats, the deployment of an appropriate defense mechanism is needed. As Fig. 1 illustrates, the defense life-cycle includes four phases: *Prevention*, *Monitoring*, *Detection*, and *Mitigation*. The prevention phase ensures that appropriate safeguards are placed in different locations to secure services and data. In the monitoring phase, monitoring tools are deployed to gather useful host or network information to follow the execution of the system. The detection phase is where an Intrusion Detection System (IDS) analyzes the running systems, looking for deviations from a pre-established normal behavior.

IDSs vary depending on whether they monitor network traffic (Network-based IDS) or local hosts (Host-based IDS) (Scarfone and Mell, 2007; Stein et al., 2005; Anuar et al., 2008; Lazarevic et al., 2003; Xiao et al., 2010). IDSs are divided into two categories: *anomaly-based* and *signature-based*. Anomaly-

* *Corresponding author.*
E-mail addresses: alireza.shameli@synchromedia.ca, alireza.shameli-sendi@polymtl.ca (A. Shameli-Sendi), mohamed.cheriet@etsmtl.ca (M. Cheriet), wahab.hamou-lhadj@concordia.ca (A. Hamou-Lhadj).
http://dx.doi.org/10.1016/j.cose.2014.04.009
0167-4048/

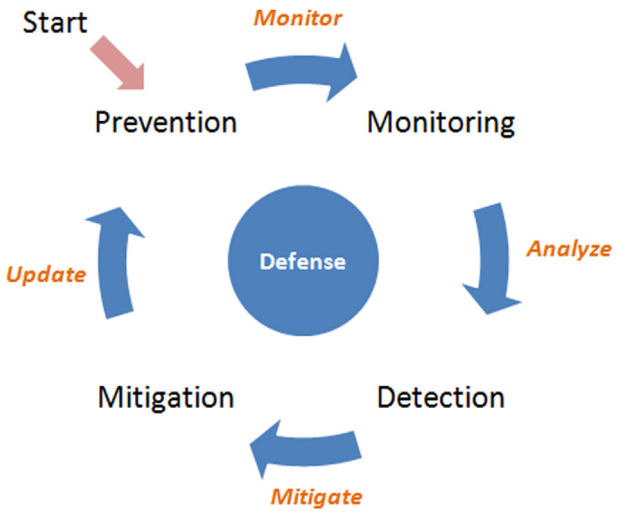

Fig. 1 – Defense life-cycle.

based techniques rely a two-step process. The first step, the training phase, a classifier is built using a machine learning algorithm, such as a decision trees, Bayesian Network, a Neural Network, etc. (Berkhin, 2001; Adetunmbi et al., 2008; Han and Kamber, 2006). The second step, the testing phase, tests the detection accuracy (by measuring true positive and false positive rates). The anomaly-based detection approach is able to detect unknown attack patterns and does not need predefined signatures. However, it suffers from the problem of characterizing the normal behavior. Signature-based techniques (also known as misuse detection) (The Snort Project, 2009), on the other hand, rely on known patterns (signatures) of attacks. Pattern matching makes this technique deterministic, which means that it can be customized for various systems, although it is difficult to find the right balance between accuracy and generality, which may lead to false negatives and false positives (Difference between Signature Based and Anomaly Based Detection in IDS; Yusof, 2009).

The last phase, mitigation, complements the defense life-cycle by evaluating the severity of attacks and selecting a correct response at the right time. In the mitigation phase, an Intrusion Response System (IRS) is responsible for selecting appropriate countermeasures to effectively handle malicious or unauthorized activities.

An IRS has to assess the value of the loss incurred by a compromised resource (Gehani and Kedem, 2004). It also has to have an accurate evaluation of the cost of the response (Strasburg et al., 2009; Stakhanova et al., 2007a). Otherwise, an automated IRS may reduce network performance, or wrongly disconnect valid users from the network. Moreover, a badly designed IRS may result in high costs associated with reestablishing the services. This incurred overhead often pushes the administrators to simply disable the IRS.

Designing an IRS poses several challenges. First, the chain of vulnerabilities exploited by an attacker can link services on either a single machine or those on different machines (Ammann et al., 2002; Jha et al., 2002). The complexity of the attack makes it a challenge to accurately calculate the risk impact. Then, there are the many decisions that an IRS needs to make, which can be summarized in the following questions:

- Is the attack harmful enough to warrant repelling?
- What is the value (importance) of the compromised target?
- Which set of responses is appropriate for repelling the attack?

Intrusion Risk Assessment (IRA) is the process of identifying and characterizing risks. The result of risk assessment helps minimize the cost of applying all available sets of responses. It may be enough in some situation to only apply a subset of available responses (Jahnke et al., 2007; Kanoun et al., 2008). That is said, risk assessment helps an IRS determine the probability that a detected anomaly is a valid attack that requires attention (in the form of a response) (Mu et al., 2008).

In this paper, we classify existing IRS and IRA design approaches. The goal is to identify the strengths and weaknesses of existing approaches. We also propose guidelines for improving IRS and IRA.

The rest of this paper is organized as follows: in Section 2, we propose our taxonomy of intrusion response and risk assessment and describe their main elements. A review of recent existing IRS and IRA is presented in Section 3. Section 4, we discuss the current state of the intrusion response and risk assessment, and suggestions for future research which can improve the current weaknesses of IRS. Finally, in Section 5, we present our conclusions.

2. A taxonomy of intrusion response systems and risk assessment

The criteria we propose for classifying IRS and IRA techniques are discussed in this section. The characteristics of the proposed taxonomy are depicted in Fig. 2. These criteria are based on extensive review of the literature:

- **Level of Automation**: An important feature of an IRS is whether it can be fully automated or requires administrator intervention after each incident.
- **Response Cost**: Knowing the power of responses to attune the response cost with attack cost plays a critical rule in IRS. The evaluation of the positive effects and negative impacts of responses are very important to identify response cost.
- **Response Time**: This criterion refers to whether the response can be applied with some delay or before the attack affects the target.
- **Adjustment Ability**: Usually, an IRS framework is run with a number of pre-estimated responses. It is very important to readjust the strength of the responses depending on the attacks.
- **Response Selection**: The task of an IRS is to choose the best possible response. Existing techniques vary in the way response selection is achieved.