Future Generation Computer Systems 29 (2013) 27–45

Contents lists available at SciVerse ScienceDirect

Future Generation Computer Systems

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

A comprehensive vulnerability based alert management approach for large networks

Humphrey Waita Njogu *, Luo Jiawei *, Jane Nduta Kiere, Damien Hanyurwimfura

College of Information Science and Engineering, Hunan University, Changsha, Hunan, China

ARTICLE INFO

Article history:
Received 1 April 2011
Received in revised form
30 March 2012
Accepted 7 April 2012
Available online 25 April 2012

Keywords:
Alert management
Alert verification
Vulnerability database
Alert correlation
Intrusion detection system

ABSTRACT

Traditional Intrusion Detection Systems (IDSs) are known for generating large volumes of alerts despite all the progress made over the last few years. The analysis of a huge number of raw alerts from large networks is often time consuming and labour intensive because the relevant alerts are usually buried under heaps of irrelevant alerts. Vulnerability based alert management approaches have received considerable attention and appear extremely promising in improving the quality of alerts. They filter out any alert that does not have a corresponding vulnerability hence enabling the analysts to focus on the important alerts. However, the existing vulnerability based approaches are still at the preliminary stage and there are some research gaps that need to be addressed. The act of validating alerts may not guarantee alerts of high quality because the validated alerts may contain huge volumes of redundant and isolated alerts. The validated alerts too lack additional information needed to enhance their meaning and semantic. In addition, the use of outdated vulnerability data may lead to poor alert verification. In this paper, we propose a fast and efficient vulnerability based approach that addresses the above issues. The proposed approach combines several known techniques in a comprehensive alert management framework in order to offer a novel solution. Our approach is effective and yields superior results in terms of improving the quality of alerts.

1. Introduction

Management of security in large networks is a challenging task because new threats and flaws are being discovered every day. In fact, the number of exploited vulnerabilities continues to rise as computer networks grow. Intrusion Detection Systems (IDSs) are used to manage network security in many organisations. They provide an extra layer of defence by gathering and analysing information in a network in order to identify possible security breaches [1]. There are two broad types of IDSs: signature based and anomaly based. The former uses a database of known attack signatures for detection while the latter uses a model of normative system behaviour and observes deviations for detection [2]. If an intrusion is detected, an IDS generates a warning known as alert or alarm.

IDSs are designed with a goal of delivering alerts of high quality to analysts. However, the traditional IDSs have not lived up to this promise. They trigger an overwhelming number of unnecessary alerts that are primarily false positives resulting from non existing intrusions. Analysing the alerts of this nature is a challenging task and therefore the alerts are prone to be misinterpreted, ignored or delayed. The important alerts are often buried and hidden among thousands of other unverified, irrelevant and low priority alerts. There are several reasons that lead IDSs to generate huge numbers of alerts such as IDS systems being unaware of the network context they are protecting [3,4]. Signature based IDSs are often run with a default set of signatures. Therefore, alerts are generated for most of the attack attempts irrespective of success or failure to exploit vulnerability in the network under consideration. In fact, signature based IDSs usually do not check the effectiveness of an attack to the local network context thus contributing to a high number of false positive alerts [2]. Further, most of the traditional IDSs have limited observation abilities in terms of network space as well as the kind of attacks they can deal with [5]. Attack evidences against network resources can be scattered over several hosts. In fact, it is a challenging issue to have an IDS with properly deployed sensors able to detect the attacker traces at different spots in the network and be able to find dependencies among them.

Research has shown that most of the damages result from vulnerabilities existing on application, services, ports and protocols of hosts and networks [6]. Fixing all the known vulnerabilities before damaging intrusions take place in order to reduce the number of alerts [7,8] may not be effective especially in large networks because of the following limitations:

- Time gap between vulnerability disclosure and the software patch released by software developers.

* Corresponding authors.
E-mail addresses: hnjogu@yahoo.com (H.W. Njogu), luojiawei@hnu.edu.cn (L. Jiawei), jayri505@yahoo.com (J.N. Kiere), hadamfr@yahoo.fr (D. Hanyurwimfura).

0167-739X/$ – see front matter © 2012 Elsevier B.V. All rights reserved.
doi:10.1016/j.future.2012.04.001

- Updating hosts from different vendors in a large network takes longer thus exposing the hosts to intruders.
- Some vulnerabilities are protocol based thus an immediate patch may not be available.

It is therefore demanding to apply vulnerability analysis to improve network security.

The vulnerability based alert management approaches are popular and extremely promising in delivering quality alerts [2,9,10]. These approaches are widely accepted and used by many researchers to improve the quality of alerts especially when processing a huge number of alerts from signature based IDSs. These approaches improve the quality of alerts by eliminating alerts with low relevance in relation to the local context of a given network. They correlate network vulnerabilities with IDS alerts and filter out the alerts that do not have a corresponding vulnerability. Therefore, the vulnerability based approaches are able to remove the need for a complicated attack step library and reduce irrelevant alerts (irrelevant alerts correspond to attacks that target a nonexistent service) [11].

Most of the vulnerability based approaches are able to produce alerts that are useful in the context of the network. However, these approaches are still at the preliminary stage and there are some research gaps that need to be addressed in order to produce better results. So far there is little attention given to the following key issues. The act of validating alerts may not guarantee alerts of high quality because the validated alerts may contain huge volumes of redundant alerts as evidently seen in several vulnerability based works such as [2,4,7,9,12–16]. Generally, the analysts who review the validated alerts may take a longer time to understand the complete security incident because it would involve evaluating each redundant alert. Consequently, the analysts may not only encounter difficulties when taking the correct decision but would also take a longer time to respond against the intrusions. In fact, it is common for attacks to produce thousands of similar alerts hence it is more useful to reduce the redundancy in the validated alerts. There is no practical use in retaining all the redundant alerts. In reference to several vulnerability based approaches such as [2,4,12–16], the validated alerts may also contain a massive number of isolated alerts that are very difficult to deal with. The presence of isolated alerts may hinder the potential of discovering the causal relationship in the validated alerts. Another challenging issue is that numerous vulnerability based approaches such as [12,13] depend on outdated vulnerability data to verify alerts hence likely to contribute to poor alert verification. New attacks and vulnerabilities in networks are discovered everyday hence the need to update the vulnerability data accordingly. In addition, the information found in the validated alerts is basic and insufficient and may not enhance the meaning and semantics of the validated alerts. In fact, the obvious alert features may not adequately describe alerts in terms of their relevance, severity, frequency and the confidence levels of their sources. Therefore, there is need to supplement the information found on the alerts to further understand the validated alerts in order to reduce the overall amount of unnecessary alerts.

The primary focus of this paper is to address the above issues in order to improve the effectiveness of vulnerability based approaches. We developed a fast and efficient approach based on several known techniques (such as alert correlation and prioritisation) in a comprehensive alert management framework in order to offer a novel solution. The contributions of this work are summarised as follows:

- Development of an alert correlation engine to reduce the huge volumes of redundant and isolated alerts contained in the validated alerts. Redundant alerts are often generated from the same intrusion event or intrusions carried out in different stages. Thus, the correlation engine helps the analysts to quickly understand the complete security incident and take the correct decision.
- Construction of comprehensive and dynamic threat profile known as Enhanced Vulnerability Assessment (EVA) data. EVA data represents all vulnerabilities present in a network. EVA data is queried to assert information about alerts and the context in which they occur thereby improving the accuracy of alerts.
- Introduction of new metrics such as alert relevance, severity, frequency and source confidence thus improving the semantics of alerts in order to offer better discriminative ability than the ordinary alert attributes when evaluating the alerts.
- Maintenance of history of alerts that contain the recent and frequent meta alerts. Generally, IDSs produce alerts that may have similar patterns manifested by features such as frequent IP addresses and ports. Therefore, the history of alerts assists in handling the incoming related alerts thus improving the processing speed.
- Application of fuzzy based reasoning to determine the interestingness of the validated alerts based on their metric values. This helps to identify the most important alerts.

The following terminologies are used in this paper:

- Vulnerability: A flaw or weakness in a system which could be exploited by intruders.
- Attack: Any malicious attempt to exploit vulnerability. An attack may be successful or not in the network under consideration.
- Relevant attack: An attack which successfully exploits a vulnerability.
- Non relevant attack: An attack which fails to successfully exploit vulnerabilities in a network.
- Attack severity: The degree of damage associated with an attack in a network.
- Alert: A warning generated by IDS on a malicious activity. An alert may be interesting or non interesting. An interesting alert represents a relevant attack. While non interesting alert represents an unsuccessful attack attempt or any other alert considered not important.
- Meta alert: Summarised information of related alerts.

The rest of the paper is organised as follows: Section 2 describes the related work. Section 3 describes the proposed approach. Section 4 discusses the experiments and performance of the proposed approach. Finally, a conclusion and suggestions for future work are given in Section 5.

2. Related work

Over the last few years, the research in intrusion detection has focused on the post processing of alerts in order to manage huge volumes of alerts generated by IDSs. In this section, we analyse several vulnerability based correlation approaches.

The traditional IDSs tend to generate too general alerts that are not network specific because of being unaware of the network context they monitor. IDSs are often run with a default set of signatures hence generate alerts for most of the intrusions irrespective of success or failure to exploit vulnerabilities in the network under consideration. According to Morin et al. [9], many alerts (especially false positives) involve actors which are inside the monitored information system and whose properties are consequently also observable. The use of vulnerability data is advocated as an important tool to reduce the noise in the alerts in order to improve the quality of alerts [9,10,13]. The vulnerability data helps to differentiate between successful and failed intrusion attempts. Identifying and eliminating failed intrusion attempts improves the quality of final alerts.

Gula [12] illustrates how vulnerability data elicits high quality alerts from a huge number of alerts that are primarily false