Available online at www.sciencedirect.com

SciVerse ScienceDirect

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

Semantic aware attack scenarios reconstruction

*Sherif Saad**, *Issa Traore*

University of Victoria, Victoria BC, Canada

Keywords:
Attack scenario
Alerts correlation
Intrusion analysis
Semantic analysis

ABSTRACT

Intrusion analysis is a resource intensive, complex and expensive process for any organization. The reconstruction of the attack scenario is an important aspect of such endeavor. We tackle in this paper several challenges overlooked by existing attack scenarios reconstruction techniques that undermine their performances. These include the ability to identify and extract novel attack patterns and the correlation of heterogeneous multisensor alerts. We propose a novel attack scenario reconstruction approach that analyzes both implicit and explicit relationships between intrusion alerts using semantic analysis and a new intrusion ontology. The proposed approach can reconstruct known and unknown attack scenarios and correlate alerts generated in multi-sensor IDS environment. Moreover, our approach can handle for the first time both novel attacks and false negative alerts generated by Intrusion Detection Systems (IDSs). Our experimental results show the potential of our approach and its advantages over previous approaches.

© 2013 Elsevier Ltd. All rights reserved.

1. Introduction

Typical intrusion detection systems (IDSs) generate low level intrusion alerts that describe individual attack events. For security administrators to take appropriate responses and design adequate defensive and preventive strategies, these low level alerts must be structured adequately and mapped into meaningful attack scenarios. The attack scenario elicits the steps and actions taken by the intruder to breach the system.

At the core of the attack scenario reconstruction process is the alert correlation, which takes a set of alerts produced by one or more IDS sensors as an input and generates a high-level view of occurring or attempted intrusions (Kruegel, 2004), by finding similarity or causality between the alerts. Each alert can be associated with a unique attack scenario execution, while several alerts can be associated with the same attack scenario (execution). Hence, there is a many-to-one relationship between alerts and attack scenario, or a crisp membership relation in clustering terminology. The attack scenario reconstruction process is complicated by the presence of false negatives and false positives which correspond to inherent limitations of the IDSs. False positives lead to incorrect attack scenarios, while false negatives (i.e. attacks missed by the IDS) either make the reconstruction of the attack scenario impossible or lead to an incomplete attack scenario.

There are three main aspects to a typical attack scenario reconstruction process: identifying related alerts, mapping an adequate subset of these alerts into a relevant attack scenario, and ordering meaningfully corresponding alerts. The first and most challenging aspect in this process is the identification of the relationships between alerts, which is necessary to identify related alerts. Four types of relationships may occur between intrusion alerts:

1. Explicit relationships, which are predefined and as such can be extracted directly from the alerts.
2. Implicit relationships, which are hidden and must be inferred using some inference rules.

* *Corresponding author.*
E-mail addresses: shsaad@ece.uvic.ca (S. Saad), itraore@engr.uvic.ca (I. Traore).
2214-2126/$ – see front matter © 2013 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.jisa.2013.08.002

3. False relationships, which are derived due to the presence of false positive alerts.
4. Missing relationships, which would have been derived if there were no false negatives.

Most of the existing attack scenario reconstruction approaches tend to focus only on explicit relationships which are relatively easy to identify. Nonetheless, existing approaches can handle only syntactic relationships, which represent only a subset of explicit relationships. We are not aware of any previous work that focused on the semantic relationships between intrusion alerts. The processing of hidden, missing, and false relationships, has largely been ignored by most of the existing approaches. These three types of relationships (i.e. hidden, missing, and false) represent the main sources of attack scenario reconstruction errors.

We propose in this work, for the first time, to improve the effectiveness of the attack scenario reconstruction process by identifying implicit relationships using semantic analysis. We use an intrusion ontology to define alert semantics, and extract implicit (as well as explicit) relationships using a set of predefined semantic inference rules. We also extend the proposed semantic model to enable the processing of missing and false relationships using environmental awareness information.

We evaluate the proposed approach using two different datasets yielding excellent performances compared to the state of the art. In the literature the ***completeness*** (also known as the true detection rate) and ***soundness*** of the alerts correlation are the most widely used metrics to evaluate attack scenario reconstruction approaches. The two metrics were proposed by Ning et al. (2002). Completeness is computed as the ratio between the number of correctly correlated alerts by the number of related alerts (i.e. that belong to the same attack scenario). Soundness is defined as the ratio between the number of correctly correlated alerts by the number of correlated alerts. The completeness metric captures how well we can correlate related alerts together while the soundness metric assesses how correctly the alerts are correlated.

The experimental evaluation of our approach yields for both datasets, soundness and completeness ranging between 96% and 100% for the sample attack scenarios considered.

In an earlier version of the current paper, presented at the 2012 Foundations and Practice of Security Symposium (Saad and Traore, 2013), we proposed the use of semantic relevance to correlate semantically related alerts. We also discussed the use of prerequisites and consequences for attack scenario reconstruction (Saad and Traore, 2012a). The current paper extends the work presented in (Saad and Traore, 2012a) by using attack impact analysis to reconstruct multistage attack scenario and detect missing attack steps (i.e. false negatives). The main contribution of this paper can be summarized by the following points:

- a novel attack scenario reconstruction technique using semantic analysis and ontology engineering;
- a new method to detect missing attack steps and mitigate the effect of false negatives.

The rest of the paper is structured as follows. In Section 2, we summarize and discuss the existing literature on attack scenario construction approaches. In Section 3, we present our intrusion semantic model and the underlying concepts and metrics. In Section 4, we start by summarizing our attack scenario reconstruction approach, and then present in detail the key steps and techniques involved in the scenario reconstruction process. In Section 5, we present our experimental study to evaluate the performance of the proposed approach. Finally, in Section 6, we make some concluding remarks and outline our future work.

2. Related works

Several attack scenario reconstruction approaches have been proposed in the literature. The proposed approaches can broadly be categorized in two different groups, specifically, knowledge-based approaches and those based on clustering and data-mining techniques. We discuss related work under each of the above categories in the following.

2.1. *Clustering and data mining-based approaches*

The first category of attack scenario reconstruction approaches use data clustering and data mining techniques, either to cluster alerts based on their attributes similarity or to mine alerts sequences in specific time interval.

Li et al., investigated multi-step attack scenario reconstruction using association rule mining algorithms (Li et al., 2007; Lei and tang Li, 2007; tang Li et al., 2007). The authors assumed that multi-step attacks often happen in a certain time interval and based on this assumption an attack sequence time window is defined and used for association rule mining. The DARPA 2000 dataset was used to evaluate the proposed approach yielding attack scenario detection rate of 92.2%.

Ding et al., proposed an attack scenario reconstruction model by extending the apriori association rule mining algorithm to handle the order of intrusion alerts occurrence (Ding et al., 2008). The authors introduced, more specifically, a time sequence apriori algorithm for mining intrusion alerts with respect to their order of appearance. The DARPA 1999 dataset was used to evaluate the proposed algorithm. The DARPA 1999 dataset was used to evaluate the proposed algorithm. The evaluation results show that the true scenario detection rate is 76% while the soundness of the approach is 53%.

Al-Mamory and Zhang proposed a lightweight attack scenario reconstruction technique by correlating IDS alerts based on their statistical similarity (Al-Mamory and Zhang, 2007). In the proposed approach, similar raw IDS alerts are grouped into meta-alert (MA) messages. An attack scenario is generated by correlating MA messages using a relation matrix (RM) that defines the similarities between every two MA messages. Using the DARPA 2000 dataset, it was shown that the completeness and the soundness of the proposed approach are 86.5% and 100%, respectively.

Attack scenario reconstruction systems that use clustering and data-mining approaches can handle large amount of IDS alerts and in general can reconstruct novel and unknown attack scenarios. They suffer, however, from several limitations. One of these limitations is the inability of the

Download English Version:

https://daneshyari.com/en/article/459045

Download Persian Version:

https://daneshyari.com/article/459045

Daneshyari.com