Computer Science Review ▮ (▮▮▮▮) ▮▮▮–▮▮▮

Contents lists available at ScienceDirect

Computer Science Review

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

Privacy issues in intrusion detection systems: A taxonomy, survey and future directions

Salman Niksefat [a], Parisa Kaghazgaran [b,*], Babak Sadeghiyan [a]

[a] APA Research Center, Amirkabir University of Technology, Tehran, Iran
[b] Texas A & M University, TX, USA

ARTICLE INFO

Article history:
Received 26 July 2016
Received in revised form 25 April 2017
Accepted 12 July 2017
Available online xxxx

Keywords:
Intrusion detection systems
IDS
Privacy
Privacy preserving intrusion detection system
IDS privacy issues

ABSTRACT

Intrusion Detection Systems (IDSs) detect potential attacks by monitoring activities in computers and networks. This monitoring is carried out by collecting and analyzing data pertaining to users and organizations. The data is collected from various sources – such as system log files or network traffic– and may contain private information. Therefore, analysis of the data by an IDS can raise multiple privacy concerns. Recently, building IDSs that consider privacy issues in their design criteria in addition to classic design objectives (such as IDS' performance and precision) has become a priority. This article proposes a taxonomy of privacy issues in IDSs which is then utilized to identify new challenges and problems in the field. In this taxonomy, we classify privacy-sensitive IDS data as input, built-in and generated data. Research prototypes are then surveyed and compared using the taxonomy. The privacy techniques used in the surveyed systems are discussed and compared based on their effects on the performance and precision of the IDS. Finally, the taxonomy and the survey are used to point out a number of areas for future research.

Contents

* Corresponding author.
E-mail addresses: niksefat@aut.ac.ir (S. Niksefat), kaghazgaran@tamu.edu (P. Kaghazgaran), basadegh@aut.ac.ir (B. Sadeghiyan).

http://dx.doi.org/10.1016/j.cosrev.2017.07.001
1574-0137/

1. Introduction

Intrusion Detection Systems (IDSs) are one of the most important defensive mechanisms in computer networks. These systems can detect and possibly prevent attacks and malicious activities which frontier security mechanisms, such as firewalls, often fail to catch.

Privacy issues in the field of computer security have been studied extensively. However, there is no universal definition of privacy. One of the most common definitions of privacy in information systems is: "the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" [1].

Many countries have passed data protection and privacy laws which secure the right of privacy of their citizens. Such privacy laws include but are not limited to the US's HIPAA [2], the EU's data protection directive [3] and Canada's PIPEDEA [4].

It is imperative that new technologies and information systems not only consider users' demands and legal requirements for privacy, but also satisfy these requirements properly.

Privacy is very important to surveillance and monitoring systems such as IDSs. To detect attacks in networks and computer systems, IDSs need to collect, store and analyze a wide scope of data. This data may contain private information and therefore the operation of an IDS may have privacy-related consequences.

In this article, we propose the first taxonomy, survey and future directions on privacy issues in IDSes.

1.1. Our contributions

A taxonomy of privacy issues in IDSs. We propose a taxonomy which is based on three sources of private data: IDS input data (e.g. network traffic, log files), IDS built-in data (e.g. attack signatures or normal profiles) and IDS generated data (e.g. alerts or reports). For each source, we specify data fields which are concerns for privacy. Privacy issues for each data source are then discussed with illustrative examples.

Survey and classification of existing privacy preserving IDSs. We survey and classify existing privacy-preserving IDSs using our proposed taxonomy (Table 1). For each work, we examine the source of the private data, privacy sensitive fields and the techniques used to address the privacy requirements.

Comparison of privacy-preserving techniques. We also discuss and compare different privacy-preserving techniques that can be used to ensure privacy in IDSs. Since these techniques address different privacy issues, it is important to know how they work and how they influence the IDS' performance and precision (false-positive and false-negative rates).

Future Directions. Finally, the taxonomy and survey are used to point towards a number of interesting areas for future research in the field.

1.2. Organization

This article is organized as follows: To better illustrate the issue of privacy in IDSs, in Section 2 we review a number of interesting cases in which preserving privacy is important. We present our proposed taxonomy of privacy issues in IDSs in Section 3. We then survey the related work based on the proposed taxonomy in Section 4, we discuss the privacy techniques used in surveyed systems and compare them based on their effects on IDS' performance and precision in Section 5, finally, challenges and future directions are presented in Section 6.

2. Motivating scenarios

One of the scenarios in which preserving privacy is of great importance is *Collaborative Intrusion Detection (CID)* [31–33]. Here, a number of IDSs wish to cooperate in order to detect distributed cyber attacks such as the spread of worms or denial-of-service attacks. Privacy concerns may arise since a single IDS's data – such as alert logs – have to be shared with other IDSs which may able to be accessed by unauthorized users. Sharing this data may risk exposing sensitive information such as intranet topology, network

Please cite this article in press as: S. Niksefat, et al., Privacy issues in intrusion detection systems: A taxonomy, survey and future directions, Computer Science Review (2017), http://dx.doi.org/10.1016/j.cosrev.2017.07.001.