論文の内容の要旨

論文題目: ENHANCED TECHNIQUES FOR DETECTION, PRIVACY PRESERVATION, AND ARCHITECTURE IN INTRUSIONS DETECTION SYSTEMS

[侵入検知システムの検出能力・プライバシ保護・アーキティクチャ強化技術]

氏名: アブデュラハマン　エム．エス．アルハルビ

Abstract

An Intrusion Detection System or IDS is a software/hardware tool used to detect unauthorized access to a computer system or network. This may take the form of attacks by skilled malicious hackers, or Script using automated tools.

An IDS is required to detect all types of malicious network traffic and computer usage. This includes network attacks against vulnerable services, data driven attacks on applications, host based attacks such as unauthorized logins and access to sensitive files.

IDSs are widely recognized and deployed in computer networks to stand against a wide variety of attacks. However, IDSs deployment raises some serious technical problems, namely low detection rate, managing of a large number of triggered alerts, and users privacy violation. These problems become worse by the fact that some commercial IDSs may generate thousands of alerts per day, and miss some real attacks at the same time. Intrusions detection, identifying the real alarms from the huge volume of alarms, and maintaining users privacy are frustrating tasks for security officers. Thus, maintaining the privacy, increasing the detection rate and reducing false alarms are critical issues in IDSs efficiency and usability.

The aim of this work is summarized as: 1) to propose a new approach based on the sequential pattern data mining to improve the detection rate of IDS systems. 2) to reduce IDSs alarms, by proposing an algorithm based on continuous and discontinuous patterns. 3) to propose revocable scheme to maintain users privacy. 4) and finally as an application of IDS, anomaly detection systems are used for security protocols environments as dynamic activities protectors.

Research background

Over the past decade, the number as well as the severity of computer attacks has significantly increased. CSO magazine conducted a survey on the 2004 cyber crimes, which shows a significant increase in reported electronic crimes. Compared to the previous year, more than 40% of intrusions and electronic crimes are reported. Also, 70% of the respondents reported at least one electronic crime or intrusion was committed against their organization. According to collected statistics, electronic crimes have an incredible impact on economy. Reports say that electronic crimes have cost more than $600 million in 2003.

In response, security services strongly recommend to deploy and implement suitable protection technology. Besides the first defense protections (e.g. firewalls, authentication, and cryptography), IDSs are recommended for attacks detection and to alert security officers for further actions. IDS has become one of the corner stones in computer security because of its triggered alarms to intrusive activities can greatly reduce the possible harm and data leakage due to attacks.

Research Motivation

Although IDSs have been deployed widely across data networks during the last decade, and their value as security components have been demonstrated. Most of them suffer from number of drawbacks namely; low detection rate, high false alarms rate, users privacy violation, and distributed IDSs secure communication. We address these potential drawbacks, that are the scope of this thesis, below.

Low detection rate and high false alarms rate: IDSs are widely recognized and deployed in computer networks to stand against a wide variety of attacks. However, IDSs deployment raises some serious technical problems, namely low detection rate and managing of a large number of triggered alerts. These two problems become worse by the fact that some commercial IDSs may generate thousands of alerts per day, and miss some real attacks at the same time. Intrusions detection and identifying the real alarms from the huge volume of alarms are frustrating tasks for security officers. Thus, increasing the detection rate and reducing false alarms are critical issues in IDSs efficiency and usability.

Users privacy violation: IDSs are used to protect computer's networks against any abuse and detect any intrusion on real time by monitoring the audit trials of the hosts and collect data about users activities and habits. This collection of data is kind of privacy threat, that makes users always worry about their related data to be revealed.

Distributed IDSs secure communication: Distributed intrusion detection systems have many elements, ranging from small agents residing in a single host to highly sophisticated analyzers receiving stream of data from hundreds of users. Some of these elements are passive and others are active. Different active IDS components are supposed to interact by dynamically sharing data, exchanging information, and using or controlling remote devices. For a given distributed IDS elements, the key question is how to secure and protect certain data residing at one of the elements, and preventing certain commands to be executed by any external element that does not have a permission.

Research Objective

As we addressed in the previous section, there are several potential drawbacks that reduce the dependency on the IDS systems. Based on that, our objective of this work is;

- to improve the detection rate of the IDS systems based on mining continuous and discontinuous patterns.
- to improve false alarms rate based on observing the behaviour of previous alarms.
- to maintain the privacy of the connected users to the network that monitored by IDS system.
- to propose an architecture so as to improve the security of different IDS elements to communicate.
- as an application we apply anomaly IDS as security protocols dynamic protector.

Contents

The structure of this thesis is as follow; In chpter1, we address the background of the IDS systems and the potential drawbacks. In chapter2, we analyze the detection techniques in IDS systems and propose a solution to improve detection. In chapter3, we propose a solution to reduce IDS generated alarms by observing the behaviour of the previous alarms generated by IDS systems. In chapter4, revocable scheme for users privacy is proposed. In chapter5, we propose an architecture to allow distributed different elements of IDSs to communicate securely. Finally, in chapter6, as an application, we apply IDS system to protect security protocols dynamically. Detailed table of contents is given below.