IDS and IPS Systems in Wireless Communication Scenarios

Adolfo Alan Sánchez Vázquez
University of Murcia, Spain

Gregorio Martínez Pérez
University of Murcia, Spain

INTRODUCTION

In principle, computers networks were conceived to share resources and certain computing devices among a select group of people working in academic institutions. In this context, the security did not have high importance. Today, through the network circulates a lot of valuable data (budgets, credit card numbers, marketing data, etc.), much of which can be considered confidential. Here is where security takes great importance—so that these data cannot be read or modified by any third party, and the services offered are always available and only to authorized people (confidentiality, integrity, and readiness).

When we refer to security, there are some terms of great importance. *Risk* is defined as any accidental or not prospective exhibition of information as consequence of the bad operation of hardware or the incorrect design of software. *Vulnerabilities* indicate when a failure in the operation of software and/or hardware elements exposes the system to penetrations. Starting from here we can define *attack* as an event against the good operation of a system, and it can be successful or not. If the attack is successful and access is obtained to the files and programs or control is obtained to the computers without being detected, then we are dealing with a *penetration.* This leads to an *intrusion,* which is a group of actions compromising the integrity, confidentiality, and readiness of computer resources (Sobh, 2006).

The main objective of this article is to explain to the reader the main concepts regarding intrusion detection systems (IDSs) and intrusion prevention systems (IPSs), and the particular issues that should be additionally considered when protecting wireless communication scenarios (in comparison with IDSs/IPSs in traditional wired networks). It also includes an extended view of the current state of the art of IDSs and IPSs in wireless networks, covering both research works done so far in this area, as well as an analysis of current open source IDSs and IPSs, and how they are dealing with the specific requirements of wireless communication networks.

This article is organized as follows: First, we start with a summary of the main related works in the *background* section; then we give a description of the important concepts of security, a classification of intrusion detection systems, and a brief comparative of the operation of IDSs in wired and wireless networks. Next, we highlight certain research works exemplifying efforts done so far in wireless scenarios. We present the main ideas behind our current research work to model intrusions in wireless scenarios, before offering future directions of work and a summary of the main ideas expressed in the article.

BACKGROUND

Many have been the efforts carried out to counteract the main weaknesses of IDSs and IPSs in wireless networks. In this sense, we can speak of different investigations directed to specific attacks in wireless scenarios by means of detection mechanisms based on artificial intelligence, design of monitoring IDSs, proactive IDSs, modeling of IDSs, and approaches based on system requirements and political issues.

Aime, Calandriello, and Lioy (2006) propose a mechanism of attack detection based on the shared monitoring of the networks by all the nodes, where one will be able to determine if the event is a bad behavior or an attack. The key idea is to install a monitor (ethereal) in each node of the network, and to produce evidence (information about the state of the network) and to share that among all the nodes. For each captured package, the system spreads a complete view of the packet headers, some general statistics are added such as timestamp, frame number, and longitude in bytes. The focus is 802.11 frames, although they are also considering source, destination, and BSSID addresses, sequence number, frame type, subtype, and retry flag. With this data, a list of events is built in each node.

We also find efforts based on anomaly detection by means of artificial neural networks, where the intrinsic characteristics and observables of the normal behavior are different from the abnormal behavior. A clear example is the proposal of Liu, Tian, and Li (2006), whose method of detection of intrusions is based on DGNN (dynamic grow-

Copyright © 2009, IGI Global, distributing in print or electronic forms without written permission of IGI Global is prohibited.

ing neural network) and consists of Hebbian learning rules to which are added new neurons under certain conditions. Three of the more common attacks in wireless networks are: war driving, MAC spoofing, and WEP cracking, and we find investigation focused on preventing this type of attack. Hsieh, Lo, Lee, and Huang (2004) developed a proactive wireless hacker detection system (WIDS) basically based on a framework that proposes an answer plan designed to prevent the user in intranets of additional damages for each attack type. The structure of this proposal consists of five modules: packet capture, session analysis, hacker detection, honeypot, and alarm modulates. Tsakountakis, Kambourakis, and Gritzalis (2007) propose a design of WIDS modules to tackle 802.11i-specific attacks. Also, it evaluates the 802.11i-enabled WIDS modules, namely WIDZ. The tests were performed utilizing the majority of well-known open source attack tools and specific attack generators. Some types of attacks were detected and others were not detected.

WIRELESS INTRUSION DETECTION AND PREVENTION SYSTEMS

Wireless networks are particularly susceptible to attacks as interception and injection, to mention just one example. The problem is inherent to wireless protocols since they use the air as its primary means of transmission. Contrary to the conventional network where the location of a network is physically limited by the infrastructure of the network, the locus for a wireless device is not limited to a connection network backplane. This represents serious problems in the moment of deploying IDS. In wireless networks, IDSs receive packages of any closer networks or next antennas; this means that the IDS may process a great quantity of malicious packages and of unknown origin. The signs in wireless networks vanish in cloud form around the access point, and the signal radiated is attenuated, allowing that, in the periphery of the cloud, a corrupted signal and certain packets originate.

The IDS based on a network (NIDS) commonly listens to the network, captures and examines the packages flowing through the same network in contrast with the firewalls; NIDS can analyze the entire packet, not just the header. It is able to look at the payload within a packet to see which particular host application is being accessed, and raise alerts when attackers try to exploit a bug in such code. NIDSs are host independent, and can run like "black box" monitors to cover entire networks. In practice, active scanning slows down the network considerably and can effectively analyze a limited bandwidth network. NIDSs often required dedicated hosts/special equipment and can be prone to the network attack (Kachirski & Guha, 2003).

The IDS based on a host (HIDS) only cares what is happening in each individual host; monitors specific files, logs, and registries installed in a single computer; and they can alert any access or modification in the object monitored (Chari & Cheng, 2003).

They are able to detect actions such as repeated failed access attempts or changes to critical system files, and normally operate by accessing log files or monitoring real-time system usage. To ensure effective operation, host IDS clients must install every host of the network, tailored to specific host configuration. Host-based IDSs do not depend on network bandwidth and are used for smaller networks, where each host dedicates processing power towards the task of system monitoring (Kachirski & Guha, 2003).

IDSs, according to their functionality, are classified in anomaly detection and misuse detection systems (Tombini, Devar, Mé, & Duccassé, 2004). Anomaly detection consists of the detection of intrusions based on the non-habitual behavior of a system or the resources of the same one. The objective is to evaluate the correct use and acceptable behavior of a certain system, pointing out any activity that is outside of this behavior. Among the more highlighted efforts in this aspect, we find the use of statistical analysis, data mining, and limitation of flow or traffic.

Misuse detection is directed to the identification of intrusions in a system by means of the establishment of static information, providing a necessary base to determine a malicious activity according to how the static information is structured. A classification is obtained that is of vital importance; a classifier trains to discriminate, being based on the data of the network traffic.

The use of wireless networks has generated important changes in the implementation of the IDS, as wireless networks are conceptually and operationally different. For the wired system, the IDSs are distributed applications analyzing events in a network system to identify malicious behavior (Vigna, Valeur, & Kemmerer, 2003). And for wireless systems, intrusion detection systems analyze events in mobile and ad hoc networks. For this reason any discussion in relation to these architectures and their operational atmospheres will allow an in-depth exploration of the important aspect to consider in the moment of displays in an effective way wireless intrusion detection systems.

Stallings (2003) shows us in the Table 1 the clear limitation of IDS systems in wireless networks.

Already mentioned were the natural risks of a wireless network, helping us to identify a series of possible attacks that put in risk the security of the information and the stability of the computational systems. Table 2 summarizes these possible attacks, found in a recent investigation by Zhong, Khoshgoftaar, and Nath (2005).

IPS

An intrusion prevention system (IPS) is a mechanism that tries to provide an automatic, efficient, quick, and exact answer

4 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/ids-ips-systems-wireless-communication/13821

Related Content

The Impact of Technological Frames on Knowledge Management Procedures
Chun-Tsung Chen (2009). *Encyclopedia of Information Communication Technology (pp. 401-412).*
www.irma-international.org/chapter/impact-technological-frames-knowledge-management/13386

Automotive Industry Information Systems: From Mass Production to Build-to-Order
Mickey Howard, Philip Powelland Richard Vidgen (2005). *Journal of Cases on Information Technology (pp. 16-30).*
www.irma-international.org/article/automotive-industry-information-systems/3145

Building a Measurement Framework for m-Government Services
Emmanouil Stiakakisand Christos K. Georgiadis (2012). *International Journal of Information Systems and Social Change (pp. 18-37).*
www.irma-international.org/article/building-measurement-framework-government-services/72331

J
(2007). *Dictionary of Information Science and Technology (pp. 376-378).*
www.irma-international.org/chapter//119571

Strategic Vision for Information Technology
Mary Elizabeth Brabston (2005). *Encyclopedia of Information Science and Technology, First Edition (pp. 2643-2647).*
www.irma-international.org/chapter/strategic-vision-information-technology/14668