Intrusion Detection: A Survey

F.Sabahi, IEEE Member
School of Computer Engineering,
Azad University,
Arak, Iran
fs_sabahi@yahoo.com

A.Movaghar, IEEE Senior Member
School of Computer Engineering,
Sharif University of Technology,
Tehran, Iran
movaghar@sharif.edu

Abstract

The rapid proliferation of computer networks has changed the prospect of network security. An easy accessibility condition cause computer network's vulnerable against several threats from hackers. Threats to networks are numerous and potentially devastating. Up to the moment, researchers have developed Intrusion Detection Systems (IDS) capable of detecting attacks in several available environments. A boundlessness of methods for misuse detection as well as anomaly detection has been applied. Many of the technologies proposed are complementary to each other, since for different kind of environments some approaches perform better than others. This paper presents a taxonomy of intrusion detection systems that is then used to survey and classify them. The taxonomy consists of the detection principle, and second of certain operational aspects of the intrusion detection system.

1. Introduction

Threats to networks are numerous and potentially devastating. Up to the moment, researchers have developed Intrusion Detection Systems (IDS) capable of detecting attacks in several available environments. A boundlessness of methods for misuse detection as well as anomaly detection has been applied. Many of the technologies proposed are complement to each other, since for different kind of environments some approaches perform better than others. IDS do it by collecting data from network and analysis of transmitted packets inside the network. But generally IDSs do not act operative reaction against occurred attacks. IDSs usually have the state of informing administrator for occurrence of an intrusion. IDSs have several methods for detect attacks. Following Processes are examples of IDS operations for detect intrusions [1, 2]:

1. Monitoring and analyzing network activities
2. Finding vulnerable parts in network
3. integrity testing of sensitive and important data

2. Data Source

IDSs typically perform extensive logging of data that is related to detected events. These data can be used to confirm the validity of alerts, investigate incidents, and correlate events between the IDS and other logging sources [8].

Host-Based: which monitors the characteristics of a single host and the events occurring within that host, for suspicious activity.

Network-Based: which monitors network traffic for particular network segments or devices and analyzes the network and application of protocol activity to identify suspicious activity [7].

Hybrid: In this type both kinds of IDS can be used simultaneously.

Network Behavior Analysis (NBA): which examines network traffic to identify threats that generate unusual traffic flows, such as distributed denial of service (DDoS) attacks, certain forms of malware, and policy violations (e.g., a client system providing network services for other systems) [8].

978-0-7695-3371-1/08 $25.00 © 2008 IEEE
DOI 10.1109/ICSNC.2008.44

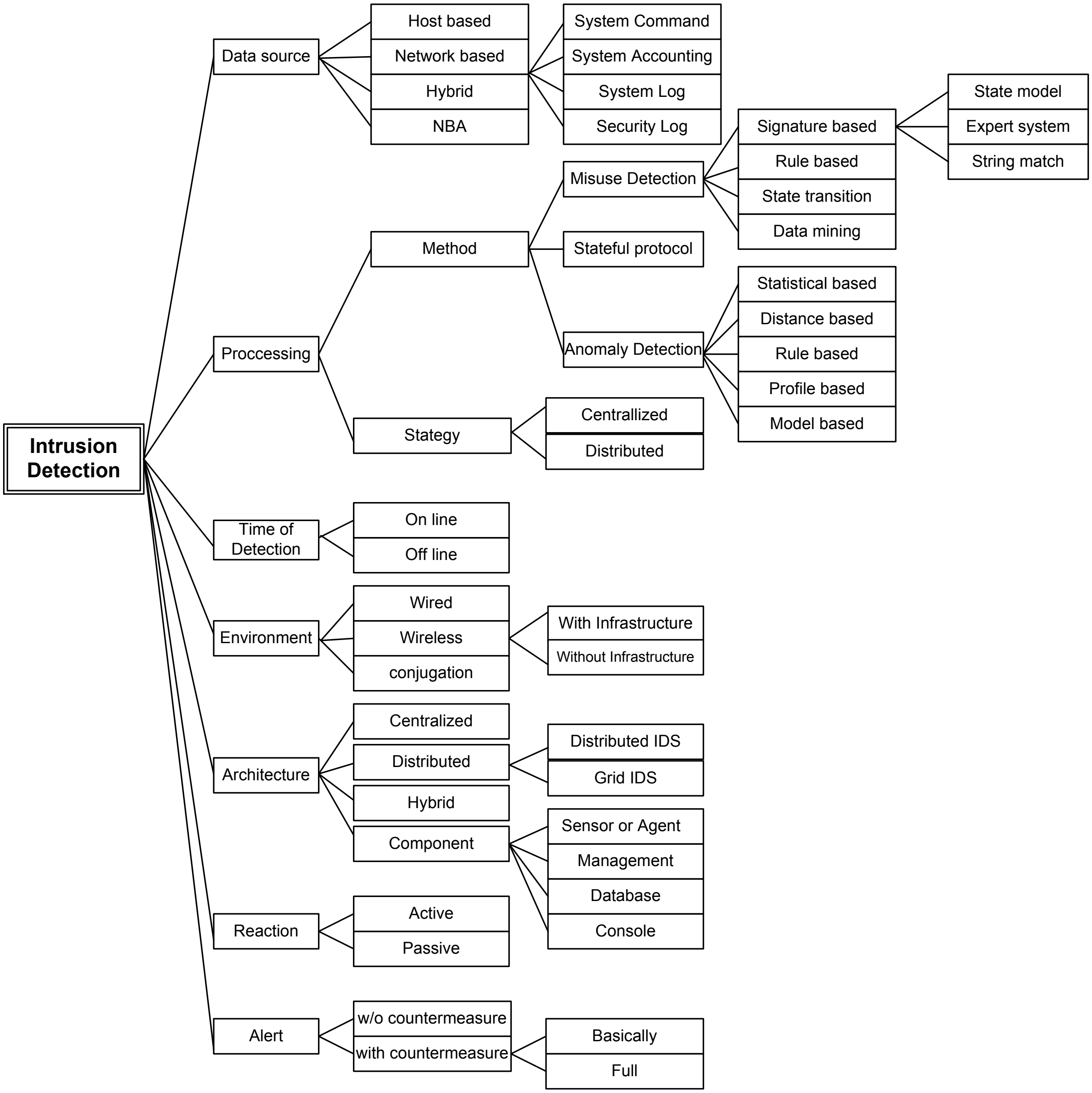

Figure 1. Taxonomy of intrusion detection systems

2.1. Resources

System command: find malicious activities by analyzing information from system commands events, IDS can find useful information for proceeding for finding intrusions in this information.

System Accounting: system accounting information may be useful for IDS but this information usually have not widely useful information and there aren't many IDS that use this information for detecting intrusion.

System log: system log files have considerable information that usable for both attackers and security systems. System logging data contain information that is not available at the network level, such as when user login and send an email [4].

Security log: the security audit trails represent records that contain all potentially important activities related to the system [4]. By analyzing these log files that created through these activities, IDS can find intruders in the network.

3. Processing of the information

Once required data collected, an IDS analysis engine processes these data in order to identify intrusive activities.

3.1. Misuse detection

The main object of misuse detection focuses to to use an expert system to identify intrusions based on a predetermined knowledge base [4].

Signature based: matching available signatures in its database with collected data from activities for identifying intrusions.

Rule based: rule based system uses a set of "if-then" implication rules to characterize computer attacks [7].

State transition: in this approach IDSs try to indentify intrusion by using a finite state machine that deduced from network. IDS states correspond to different states of the network and an event make transit in this finite state machine. An activity identifies intrusion if state transitions in the finite state machine of network reflect to sequel state.

3.2. Stateful protocol analysis

This method compares predetermined profiles of generally accepted definitions of benign protocol activity for each protocol state against observed events to identify deviations [8].

3.3. Anomaly Detection

This method works by using the definition "anomalies are not normal". There are many anomaly detection that proposed algorithms with differences in the information used for analysis and according to methods that are employed to detect deviations from normal behavior. But the most important object is the anomaly detector that must be able to distinguish between the anomaly and normal behavior properly.

Statistical based methods: statistical methods monitor the user/network behavior by measuring certain variables statistics over time [7].

Distance based methods: these methods try to overcome limitations of statistical outlier detection approach when the data are difficult to estimate in the multidimensional distributions. [8]

Rule based: in rule based systems, IDSs have defined the knowledge of normal behavior of user/network and identified intrusion by comparison this predefined normal behavior with user/network current activities.

Profile based methods: this method is similar to rule based method but in this type, profile of normal behavior is built for different types of network traffics, users, and all devices and deviance from these profiles means intrusion.

Model based methods: other approaches based on deviance normal and abnormal behavior is modeling them but without creating several profile for them [8]. In model based methods, researchers attempt to model the normal and/or abnormal behaviors and deviation from this model means intrusion.

4. Time of Detection

In time aspects consideration, IDSs have two main groups: online IDS that tries to detect intrusion in real time (or near real-time) and off-line IDS that performs post-analysis data for detecting intrusions [7].

5. Environment

Easy accessibility condition in this kind of networks causes their vulnerability against wired networks to high. The level of vulnerability has made it necessary to consider security issues in wireless networks more than before and nowadays new group added to IDS categories for Wireless networks that named WIDS (Wireless Intrusion Detection System). WIDS which monitors wireless network traffics and analyze them to identify suspicious activity involving the wireless networking protocols.

Wireless network have two main groups: with infrastructure (e.g. WLAN) and without infrastructure (e.g. Adhoc). Intrusion Detection in wireless networks with infrastructure is similar to regular IDS that exist in wired network. But in wireless network without infrastructure has different situation for performing security issues, because in these types of wireless networks there are specific protocols used in them that challenge regular IDS to work properly in networks with these protocols. In this kind of wireless networks, detecting intrusion differ from wireless networks with infrastructure because tasks perform distributed frequently and necessary to improve regular IDS methods for these types of wireless networks.

6. Architecture

Most intrusion detection systems are centralized architecture and detect intrusions that occur in a single monitored system/network [16]. But nowadays several attacks appear that have distributed architecture and centralized processors are not able to process collected data from massive network or distributed attacks (e.g. DDoS).

In centralized IDS, the analysis of data is performed on a fixed number of locations. But in distributed IDS (DIDS) the analysis of data is performed on a number of locations that is commensurate to number of available systems in network. In wireless network without infrastructure we force to use DIDS because we can't set a fixed location/host for using centralized IDS. Recently, New methods appear in distributed IDS categories with name GIDS (Grid Intrusion Detection system), which uses Grid computing resources to detect intrusion packets [6].

The example of typical architecture is shown in figure 2. The *sensors/agents* components monitor and analyze activities. A *management server* is a centralized device that receives information from the sensors or agents and manages them. A *database server* is a repository for event information recorded by sensors, agents, and/or management servers. A *console* is a program that provides an interface for the IDS's users and administrators [8].

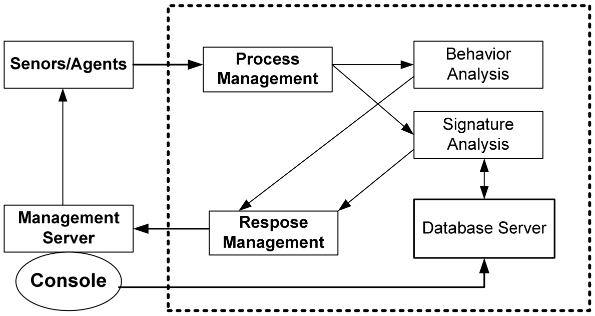

Figure 2. Taxonomy of intrusion detection systems

7. Reaction and Alert

Regularly, IDSs react against attacks passively [9]. IDSs have passive reaction and simply inform administrator of a malicious event, without any countermeasure. In passive reaction, the most important issue is the speed of notification when attacks occur in network [10]. IDSs also beget an active reaction when attacks occur and response to critical events. But active IDSs generally don't act perfect countermeasure against intrusion because with doing that, IDSs need more process resources and concentrate on detecting and counter measuring capabilities in one system that is not recommended at all [11,12].

8. Conclusion

It is not realistic to except that an IDS be capable to detect all attacks. Perfect detection is simply not an attainable goal given the complexity and rapid evolution in both attacks and systems. In this paper, we provide an overview of intrusion detection techniques and methods. We review a brief survey of IDS taxonomies without in-depth details. We sure this brief survey is useful for all researchers that want to investigate more efficient methods against intrusions.

9. References

[1] J. Rittinghouse and J. Ransome, *Wireless Operational Security*, Digital Press, 2004, ch.9.

[2] S. Northcutt and J. Novak, *Network Intrusion Detection: an Analyst's Handbook*, 2ed ed., New Riders, 2000.

[3] P. Kabiri and A.A. Ghorbani, "Research on Intrusion Detection and Response: A Survey," *Int. Journal of Network Security*, vol.1, No.2, pp. 84-102, 2005.

[4] D. J. Brown, B. Suckow, and T. Wang, "A Survey of Intrusion Detection Systems," 2002.

[5] A.K. Jones and R.S. Sielken," Computer system Intrusion Detection: A Survey," Department of Computer Science, University of Virginia, 2000.

[6] F.Y. Leu, J.C. Lin, M.C. Li, C.T Yang, P.C Shih, "Integrating Grid with Intrusion Detection," *Proc. 19th International Conference on Advanced Information Networking and Applications*, pp. 304-309, 2005.

[7] White paper, "Intrusion Detection: A Survey," ch.2, DAAD19-01, NSF, 2002.

[8] K. Scarfone, P. Mell, "Guide to Intrusion Detection and Prevention Systems (IDPS)," NIST Special Publication 800-94, Feb. 2007.

[9] T. Wang and X.D. Yang, "IntruDetector: A Software Platform for Testing Network Intrusion Detection Algorithms," 2001.

[10] M.E. Kuhl, M. Sudit, J. Kistner, and K. Costantini, "Cyber attack modeling and simulation for network security analysis," *IEEE Simulation Conf.*, pp. 1180-1188, Dec. 2007.

[11] M. Blanc, J. Briffaut, P. Clemente, M. Gad El, and Rab C. Toinard, "A Collaborative Approach for Access Control, Intrusion Detection and Security Testing," IEEE Infocom 2006.

[12] K.L. Ingham, "Anomaly Detection for HTTP Intrusion Detection: Algorithm Comparison and the Effect of generalization on Accuracy," Ph.D. dissertation, Univ. of New Mexico, Albuquerque, 2007.