Autonomic Agent-Based Self-Managed Intrusion Detection and Prevention System

A. Patel[1], Q. Qassim[1], Z. Shukor[1], J. Nogueira[2], J. Júnior[3] and C. Wills[4]

[1]Department of Computer Science, Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia, 43600 Bangi, Selangor Darul Ehsan, Malaysia
e-mail: apatel@ftsm.ukm.my; qaisjanabi@gmail.com; zs@ftsm.ukm.my
[2]Setor Técnico-Científico – Criminalística, SETEC/SR/DPF/CE, Departamento de Polícia Federal
e-mail: helano@apcf.org.br
[3]Network Computer Laboratory, LARCES / UECE, State University of Ceara
e-mail: celestino@uece.br
[4]Faculty of Computing Information Systems and Mathematics, Kingston University, United Kingdom
email: ccwills@kingston.ac.uk

Abstract

Over the last fifteen years the world has experienced a wide variety of computer threats and general computer security problems. As communication advances and information management systems become more and more powerful and distributed, organizations are becoming increasingly vulnerable to potential security threats such as intrusions at all levels of Information Communication Technology (ICT). There is an urgency to provide secure and safe information security system through the use of firewalls, Intrusion Detection Systems (IDSs), Intrusion Prevention Systems (IPSs), encryption, authentication, and other hardware and software solutions. Many intrusion detection and prevention systems have been designed, but still there are significant drawbacks. Some of these drawbacks are low detection efficiency, inaccurate prevention schemes and high false alarm rates. Since IDSs and IPSs have become necessary security tools for detecting and preventing attacks on ICT resources, it is essential to upgrade the previous designs, techniques and methods to overcome flaws. Anomaly detection is an essential component of the detection mechanism against unknown attacks but this requires advanced techniques to be better and more effective. In this paper we put forward a new agent-based self-managed approach of anomaly intrusion prevention system based on risk assessment and managed by the principles of the Autonomic Computing (AC) concept, which has all the flavors of self-management. Applying AC will open up new frontiers, and enhance and improve the intrusion detection mechanism by not only protecting the system's information and assets but also to stop and prevent the breach before it happens. It can also assist in digital forensics and investigations.

Keywords

Information Security, Intrusion detection, Intrusion Prevention, Anomaly Detection, Misuse Detection, Autonomic Computing, Self-Management.

1. Introduction

The problem of managing and protecting information has existed long before information and communication technology came into being. However, as technology advances and information management systems become more and more complicated, the problem of enforcing information security also becomes more critical. The widespread use of communication networks for all purposes of computing is posing new serious security threats and increases the potential damage that security violations may cause. As organizations' use of and reliance upon information increases, so too does their reliance on computer network and distributed computing environments, which become more vulnerable to security breaches. This reliance requires advanced, intelligent, secure and safe information security systems to protect the organization's assets and information, in autonomic and intelligent ways. As information management systems become more and more powerful and distributed, the number of threats grows and diversifies. Since the inability of misuse detection to detect novel attacks that have no signatures yet has stimulated the need for the investigation set out in this paper. This paper puts forward a new approach for anomaly intrusion detection/prevention system based on autonomous agents which are managed by the fundamental principles and concepts of autonomic computing. These allow for self-management such as self-configuring, self-optimization, self-detection, self-protection, self-prevention and self-healing. Autonomic computing dramatically improves the detection performance and enables the development of the knowledge-base of new detected attacks reducing both false and actual alarm rates.

In Section II of the paper we briefly outline important concepts that are used throughout this paper. Section III outlines the most significant limitations in existing intrusion detection and prevention methods and describes the desired characteristics of an intrusion detection/prevention system. In Section IV we propose a solution that can help to overcome the limitations in existing intrusion detection/prevention systems by suggesting a new autonomous agent-based self-managed approach of anomaly intrusion prevention system. Section V briefly discusses and concludes the paper with indications of our future work.

2. Background and Concepts

This section provides a brief introduction to the important concepts that are used throughout this paper as well as present the motivations behind the philosophy in approaching, designing and developing smart detection and prevention systems.

2.1. Intrusions

Intrusions are actions that attempt to bypass security mechanisms of computer systems in non-obvious ways (Bidgoli, 2006). They are any set of actions that threatens the integrity, availability, and/or confidentiality of the information. Confidentiality means that information is not made available or disclosed to unauthorized individuals, entities or processes. Integrity means that data has not been altered or destroyed in an unauthorized manner and availability means that a system that has the required data ensures that it is accessible and usable upon demand by an

authorized system user (Whitman and Mattord, 2005). Frequently, intrusions are caused by an outside attacker accessing the system from the Internet or local network or the operating system of the infected machine or uses the security flaw of a third-party application (middleware), or by inside attackers who may be authorized users in some respects attempting to gain and misuse non-authorized security and system privileges.

2.2. Intrusion Detection (ID)

Intrusion detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents (Newman et al., 2004), which are real violations or imminent threats of violation of computer security policies and standard security practices. Incidents have many causes, such as malware, attackers gaining unauthorized access to systems from the Internet, and authorized users of systems who misuse their privileges or attempt to gain additional privileges for which they are not authorized. Although many incidents are malicious in nature, many others are not. For example, a person might mistype the address of a computer and accidentally attempt to connect to a different system without authorization. There are two basic techniques used to detect intruders: anomaly detection and misuse detection (Bringas and Penya, 2009), (Jiang and Chang, 2009).

Anomaly Detection is designed to uncover abnormal patterns of behavior. It establishes a baseline of normal usage patterns, and anything that widely deviates from it gets flagged as a possible intrusion. It is an extremely powerful and novel tool but a potential drawback is the high false alarm rate which can cause inadvertent system behavior.

Misuse Detection is also known as signature detection. Here each instance in a data set is labeled as “normal” or “intrusive” and a learning algorithm is trained over the labeled data over a period of time until some level of stability is reached. These techniques are able automatically to retrain the intrusion detection mechanisms and update the Knowledge Base System (KBS) with different input data that include new types of attacks. The KBS has high degree of accuracy in detecting known attacks and their variants. Its disadvantage is that it cannot detect unknown intrusions that are new and not yet recorded in the KBS. It relies on human experts to extract or compose signatures and insert in the KBS. This method uses specifically known patterns of unauthorized behavior to predict and detect subsequent similar attempts. These specific patterns are commonly called signatures, or alternatively footprint matching.

2.3. Intrusion Prevention (IP)

Intrusion Prevention is the act of stopping detected bad data set in real-time by not allowing it to execute or continue to its destination (Scarfone and Mell, 2007). It is useful against denial of service floods, brute force attacks, vulnerability detection, protocols anomaly detection and prevention against unknown exploits within the kernel Operating System or middleware and networking applications.

2.4. Intrusion Detection and Prevention Systems (ID/PSs)

Intrusion detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents. An intrusion detection system (IDS) (Martin, 2009) is a device or software application that monitors network and/or information system for malicious activities or policy violations and response to that suspicious activity by warning the system administrator or the process acting on its behalf by one of several ways, which includes displaying an alert, logging the event or even paging the administrator or the acting process.

Intrusion prevention is the process of performing intrusion detection and stopping known attacks in an instant or attempting to stop detected possible incidents by quarantining or isolation. The Intrusion Prevention System (IPS) (Martin, 2009) is a device or software application that complements IDS and it has all the capabilities to stop possible incidents from occurring against known attacks. IPS is designed and developed for more active protection to improve upon simple IDS and other traditional security solutions. An intrusion prevention system is definitely an advanced capability adjunct to just the simple IPS. It is the next level of security technology that provides security at all system levels from the operating system kernel to network data flows to data bases (Zhou and Fang, 2009). IPS is designed to protect information systems from unauthorized access, damage and disruption, while an IDS informs of a potential attack, an IPS makes attempts to stop it (Huebscher and McCann, 2008). Another huge leap over IDS is that IPS has the capability of being able to prevent not only known intrusion signatures but also some unknown attacks due to its KBS of generic attack behaviors and interpreters.

A common attribute of IDS and IPS (ID/PS) is that they cannot provide completely 100% accurate detection. When an ID/PS incorrectly identifies benign activity as being malicious, a false positive has occurred, and when an ID/PS fails to identify malicious activity, a false negative has occurred (Martin, 2009). It is not possible to eliminate all false positives and negatives; in most cases, reducing the occurrences of one increases the occurrences of the other. Many organizations choose to decrease false negatives at the cost of increasing false positives, which means that more malicious events are detected but more analysis resources are needed to differentiate false positives from true malicious events. This is a hotly contested research topic area.

2.5. Autonomic Computing (AC)

AC is a concept borrowed from biology and applied to many fields of computing with the purpose of creating computing systems that are self-managing (Dale Kutnick et al., 2001). AC seeks to improve computing systems with the aim of decreasing or eliminating human involvement altogether through automatic system processes. The term “autonomic” comes from biology. In the human body, the autonomic nervous system takes care of unconscious reflexes, that is, bodily functions that do not require our active attention or involvement. For example bodily adjustments such as the size of the pupil, the digestive functions of the stomach and

intestines, the rate and depth of respiration, and dilatation or constriction of the blood vessels take place transparently and non-obtrusively. Without the autonomic nervous system, we would be constantly busy consciously adapting our body to its needs and to the environment. An AC attempts to intervene in computing systems in a similar fashion as its biological counterpart (Xu et al., 2004).

2.5.1. Self-Management Properties

The main properties of self-management are self-configuration, self-optimization, self-healing, and self-protection as defined in (Kephart and Chess, 2003) and (Bantz et al., 2003):

Self-Configuration: An AC system configures itself according to high-level goals, that is, by specifying what is desired, not necessarily how to accomplish it. This can mean being able to install and set it up based on the needs of the system platform and the user.

Self-Optimization: An AC system optimizes its use of resources. It may decide to initiate a change to the system proactively (as opposed to reactive or post-active behavior) in an attempt to improve performance or quality of service.

Self-Healing: An AC system detects and diagnoses problems. The types of problems that are detected can be interpreted broadly as: they can be as low-level as bit-errors in a memory chip (hardware failure) or as high-level as an erroneous entry in a directory service (software problem). If possible, it should attempt to correct the problem, for example by switching to a redundant component or by downloading and installing software updates. This is known as self-fixing. However, it is important that as a result of the healing process the system is not further harmed, for example by the introduction of new bugs or the loss of vital system settings or over use of system resources. Fault-tolerance is an important aspect of self-healing to impose a degree of tolerance which permits operation in degrade mode until they system if fully upgraded to overcome the problem. That is, an AC system is said to be reactive to failures or early signs of a possible failure as a precautionary measure.

Self-Protection: An AC system protects itself from self-distraction through malicious attacks but also from end users who inadvertently make software changes such as deleting an important file by accident. The system autonomously and automatically tunes itself to achieve security, privacy and data protection against a set of profile based on trust. Security is an important aspect of self-protection, not just in software, but also in hardware. A system may also be able to anticipate security breaches and prevent them from occurring in the first place. Thus, the AC exhibits proactive features.

2.5.2. The MAPE-K Autonomic Loop Architecture

To achieve autonomic computing, IBM has suggested a reference model for autonomic control loops (Dale Kutnick et al., 2001), which is called the MAPE-K (Monitor, Analyze, Plan, Execute, Knowledge) loop and is depicted in Figure 1. This

model is being used more and more to communicate the architectural aspects of autonomic systems. Like-wise it is a clear way to identify and classify much of the work that is being carried out in the field. In the MAPE-K autonomic loop, the managed element represents any software or hardware resource that is given autonomic behavior by coupling it with an autonomic manager. Thus, the managed element can for example be a web server, a database, a specific software component in an application, an operating system, a stack of hard drives, a wired or wireless network, a CPU, a printer, etc. Sensors, often called probes or gauges, collect information about the managed element. For a Web server, that could include the response time to client requests, network and disk usage, CPU and memory utilization. Effectors carry out changes to the managed element by transmitting signals to make adjustments or take precautions.

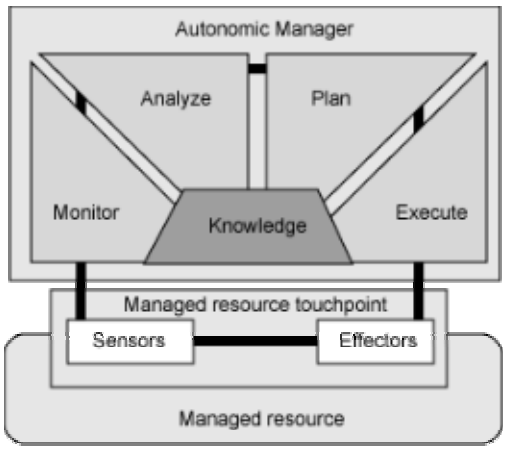

Figure 1 The MAPE-K Model (Dale Kutnick et al., 2001)

The data collected by the sensors allows the autonomic manager to monitor the managed element and execute changes through effectors. The autonomic manager is a software component that ideally can be configured by human administrators using high-level policy goals and uses the monitored data from sensors and internal knowledge of the system to plan and execute, based on these high-level policy goals for low-level operational actions that are necessary to achieve these goals. The internal knowledge of the system is an architectural model of the managed element.

3. Problem Statement

Since the number of attacks and vulnerabilities are rising, and because of the inability of misuse detection functions to detect novel attacks that have no signatures yet, researchers are looking to promote the intrusion detection mechanism to be able to detect novel attacks using anomaly detection.

3.1. Limitations of Current Anomaly Detection/Prevention Systems

Anomaly detection is an important problem that has been researched within diverse research areas. The main limitation is that it may not be able to describe what an attack is and may have high false positive rate. The disadvantages of the current anomaly detection/prevention are as follow (Deri et al., 2003):

- Anomaly detection produces usually large number of false-positive alarms, which are events signaling an IDS to produce an alarm when no attack has taken place.
- A legitimate system behavior may also be recognized as abnormal patterns. Since normal behavior can change easily and readily, anomaly-based IDS systems are prone to false positives where attacks may be reported based on changes to the "normal" rather than representing real attacks,
- Anomaly detection approach requires extensive training sets of the protected system normal activities in order to characterize normal behavior patterns. Once the training sets are defined, they need to be fed into the anomaly detection engine to create a model of the normal system usage. Therefore, any change in the system, has to relearn new patterns of behavior by updating the knowledge-base system.
- In spite of its performance, anomaly intrusion detection system in general can be immolated/disabled by the intruder through learning how and where it works in the system.
- Intrusion prevention systems can respond to a detected threat by attempting to prevent it from succeeding. They may use several response techniques which will stop the attack itself or may change its content. Either way the results will be adverse if the IPS incorrectly identifies a significant legitimate activity as being malicious.

3.2. Evaluation of Some Existing Intrusion Detection/Prevetion Systems

Studies have shown that self-managed behavior of agents can be very useful in the intrusion detection field. In an agent-based intrusion detection and prevention system specific agents can be designed and implemented in a distributed fashion. Failure in one agent may not degrade the overall detection performance of the system. Even with the vast advantages of multi-agent technology it has several weaknesses. One of the main drawbacks of this technology is the self defense strategy. Although the role of IDS is to monitor and ensure security of the protected system, the IDS itself is a primary target of the attacks. It is important for IDS agents to operate in hostile environments and continue to exhibit a high degree of fault-tolerance and performance. A major consideration of this work is to present an architecture that provides agents protection through the self-healing and self-protection properties of the autonomic computing. The following are some of the research that has been done in the area of multi-agent intrusion detection system.

Barika et al (2009) presented an agent-based intrusion detection system based on misuse detection. He outlines the use of agent technology in intrusion detection which has practical advantages. The evaluation results show that agent intrusion

detection systems do not only perform better in terms of effectiveness but also in terms of detection delay. The major drawback of the work is the inability to detect novel attacks, new threat which does not have signatures yet.

Sodiya (2006) presented a multi-level agent-based intrusion detection system, showing that applying agent-based technology to intrusion detection system provides effective malicious detection; the system was able to detect most of the intrusive events. The experimental results have shown that agent-based technology is an efficient tool for building intrusion detection system infrastructure. Although the system faces some shortcomings such as the detection process is slow, the effective detection of autonomous attacks is still very low. Another major problem is protecting the security system from attacks, since the role of IDS is to monitor and ensure security of the protected system, the IDS itself is primary target of the attacks.

Wasniowski (2005) proposed a fuzzy agent-based intrusion detection system based on multi-sensors, where agents use data from multiple sensors with a fuzzy logic to process log files. He drew attention towards how Agents represent a new generation of computing systems and are one of the more recent developments in Intrusion Detection Technology. He also explained how agents can reduce the intrusion detection workload by sifting through large amounts of data for evidence gathering. The experimental results show that the Fuzzy agent IDS is more effective than the current IDSs. The proposed architecture allows local analysis and sharing of results and as well as minimizing the communication costs, The only disadvantage of this approach is the existence of a control center carrying out the major part of the intrusion detection.

Xu et al (2004) proposed an autonomic computing architecture for defense in depth information assurance system in a way that the increasing of complexity of the system can be tackled by distributed autonomous security subsystem with the ability of self-configuration, self-optimization, self-healing and self-protection. The system has shown an enormous improvement on the defense in depth information assurance system. The main shortcoming of the work is lacking the consideration on risk evaluation and risk assessment.

3.3. Desired Characteristics of an Intrusion Detection/Prevention System

In order to satisfy its functions and to perform safe and total security against serious attacks, the ideal intrusion detection and prevention system should have the following characteristics:

- It should work in real-time, and should detect intrusions either while they are happening or shortly afterwards.
- It should recognize all or most intrusions with minimum number of false-positive alarms.
- It should run continuously with minimum human supervision.
- It should be fault tolerant in the sense that it must be able to recover from system crashes, either accidental or caused by malicious activities.

- The intrusion detection system should be able to monitor itself and detect if it has been modified by an attacker.
- It should be able to be configured according to the security policies of the system that is being monitored.
- It should be able to adapt to changes in system and user behavior over time (changes like, new applications being installed, uses changing from one activity to another or new resources being available that cause changes in system resource usage patterns).

Although these characteristics appear compelling, they have not been available yet, nor are they likely to result from other traditional security systems.

4. Solution Overview of AC Based ID/IP System

To solve the limitations identified and discussed in the previous section, we propose an anomaly prevention system based on risk analysis and inspired by the human nervous system. The human nervous system has many properties that not only allow it to take care of unconscious reflexes, that is, bodily functions that do not require our attention, but they also provide fault-tolerance in the system. The nervous system can remain functional even when many of its sensors have failed. As in the nervous system, the proposed anomaly prevention system uses small, independent, and intelligent intrusion detectors as sensors (defined as agents in this paper) as shown in Figure 2. The intrusion prevention system lies inside the host and monitors its resources (such as application activities, system calls, file access and modifications, etc) for suspicious activities. The role of the nerves like intrusion prevention is to manage these autonomous agents by providing them a high-level control commands such as indication to start or stop execution or to change some operating parameters from other entities, and to provide a set of prevention rules that will attempt to stop the attack before it happens. Since agents are independently-running entities, they can be added and removed from the protected system without altering or affecting other components, and without having to restart the intrusion prevention system. Furthermore agents may provide mechanisms for reconfiguring them at runtime without even having to restart them to achieve the continuous running with minimum human intervention. Additionally, an agent may also be part of a group that can perform different functions but also can exchange information and derive more complex results that any one of them may be able to obtain on their own. With the self-management properties the system can:

- Dynamically adapt to changing environments. With the self-configuring property it can detect hardware and/or software changes automatically and seamlessly.
- Monitor and tune resources automatically. With the self-optimizing property it can interface with other intrusion prevention systems to exchange data and files.
- Discover, diagnose and react to disruptions automatically. With the self-healing property it has the capability of self-correction when a process fails, the errors are identified and processes rerun without human intervention.

- Anticipate detection, identification and protection against threats. With the self-protecting property it can detect security incidents as they occur and take corrective actions to make it less vulnerable.

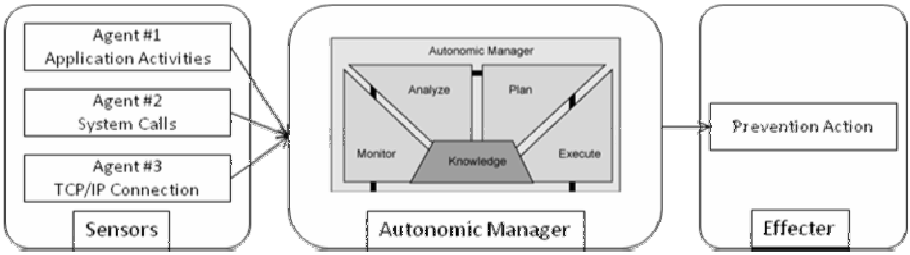

Figure 2 Agent-based Self-managed Intrusion Detection and Prevention

From the proposed solution it is shown that an intrusion prevention system whose data collection and analysis elements are operated by autonomous agents based on risk assessment and managed by AC concept with self-management properties solves most of the limitations of current intrusion detection and prevention systems more effectively with minimum human intervention. The main goal of using autonomic computing is to create computing systems capable of managing themselves to a far greater extent when given high-level objectives, and to provide set of prevention rules that will attempt to stop the attack before it happens depending on risk analysis and risk assessment. These will help to confirm the validity of the alerts and identify the false positive alerts, by measuring the risk caused by the detected threat. We can then judge whether it is a normal activity or not. To achieve the desired characteristics and grading the self-management behavior to the system, the proposed autonomic management model will be organized into six layers as shown in Figure 3. Each layer has functionalities and specific services. The top of the pyramid (Layer 6) addresses the integrated autonomic interface. This interface is the unique contact point of the user with the autonomic architecture. This is the place where strategies and policies are defined by the user. The base (Layer 1) addresses the operational manager that manages number of autonomous agents (intrusion detectors) which monitor system resources of any existence of incidents. The middle of the pyramid

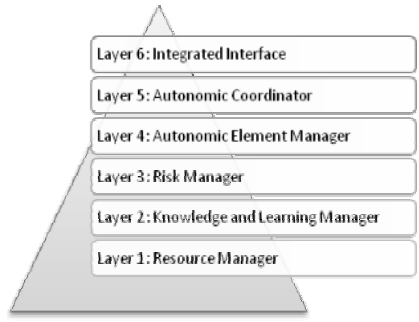

Figure 3 Management Layers in the Proposed Solution

(Layers 2, 3, 4 and 5) addresses the knowledge and learning manager that controls all the knowledge repositories and the deduction module; the risk manager that evaluate and analyze the risk of the detected threat according to strategies and guidelines provided by system administrator through Layer 6; the autonomic elements manager that manages each autonomic component (self-configuration, self-optimization, self-healing, and self-protection) individually; and the autonomic coordinator that harmonizes all the autonomic components together.

5. Discussion, Conclusion and Future recommendation

As computer and information system attacks become more and more sophisticated, the need to provide effective intrusion detection and prevention methods increases. The current intrusion detection and prevention systems have some limitations and drawbacks. The deficiency of centralized intrusion detection and prevention systems leads to the idea of deploying distributed autonomous agents based on autonomic principles. Agents are autonomous software that can act independent from one another and perform different tasks in a collaborative manner. Self configuring is responsible for ensuring overall system management is coordinated and synchronized by these agents. In addition since agents behave independently, also reconfiguration of sensors is usually difficult but through collaboration and coordination management it can be simplified and made effective.

In this paper we proposed a solution that is more effective than current intrusion detection and prevention systems. The proposed solution will provide an intelligent fault tolerant self-managed intrusion prevention system with continuous runtime and minimum human intervention due to the use of multi-agents supervised by autonomic manager, with minimum number of false-positive alarms due to the use of risk analysis and risk assessment. With the self-management properties the system can dynamically adapt to changing environments, monitor and tune resources automatically, discover, diagnose and react to disruptions automatically.

Our future plan is to extend this idea by implementing it with the use of mobile agents which have the capabilities to autonomously incarnate, migrate and consolidate inside the network from host to host to detect intrusions and execute prevention as a total solution against all known and some unknown generic threats. Another possible future work is to monitor not only the host resources but also the entire network by distributing these agents in a roving manner to make network-based intrusion prevention system to deliver maximum security by anticipating threats as and when they happen.

6. References

Bantz, Bisdikian, Challener, Karidis, Mastrianni, Mohindra, Shea and Vanover. "Autonomic Personal Computing." IBM Systems Journal 42, no. 1 (2003): 165-76.

Barika, F., Kadhi, N. E. & Ghédira, K. (2009) Agent IDS based on Misuse Approach. Journal of Software, 4, 495-507.

Bidgoli, Hossein. Handbook of Information Security. 3 vols. Vol. 3: John Wiley & Sons, Inc, 2006.

Bringas, Pablo García, and Yoseba K. Penya. "Next-Generation Misuse and Anomaly Prevention System." In Enterprise Information Systems, edited by Joaquim Filipe and José Cordeiro, 117-29: Springer Berlin Heidelberg, 2009.

Dale Kutnick, William Zachmann, Val Sribar, Jack Gold, and David Cearley. "Ibm Advances toward Autonomic Computing." edited by Lon Levitan: IBM Press, 2001.

Deri, Luca, Stefano Suin, and Gaia Maselli. "Design and Implementation of an Anomaly Detection System: An Empirical Approach." Paper presented at the Terena Networking Conference 2003.

Huebscher, Markus C., and JULIE A. Mccann. "Asurvey of Autonomic Computing — Degrees, Models, and Applications." ACM Computing Surveys 40, no. 3 (2008).

Jiang, Yaping, and Junlin Chang. "Intrusion Prevention System Base on Immune Vaccination." IEEE Computer Society (2009): 350-53

Kephart, and Chess. "The Vision of Autonomic Computing." IEEE Computer Society 36, no. 1 (2003): 41-50.

Martin, Chris. "What Is Ips and How Intrusion Prevention System Works." aboutonlinetips.com, 2009.

Newman, Daniel, Kristina M. Manalo, and Ed Tittel. Intrusion Detection Overview: John Wiley & Sons, Inc., 2004.

Scarfone, Karen, and Peter Mell. "Guide to Intrusion Detection and Prevention Systems (Idps) " In Recommendations of the National Institute of Standards and Technology National Institute of Standards and Technology 2007.

Sodiya, A. S. (2006) Multi-level and Secured Agent-based Intrusion Detection System. Journal of Computing and Information Technology, 14, 217-223.

Wasniowski, R. A. (2005) Multi-sensor agent-based intrusion detection system. Information security curriculum development. Kennesaw, Georgia ACM.

Whitman, Michael E., and Herbert J. Mattord. Principles of Information Security. Second ed: Thomson, 2005.

Xu, Xin, Zunguo Huang, and Lei Xuan. "Autonomic Computing for Defense-in-Depth Information Assurance: Architecture and a Case Study." Springer-Verlag Heidelberg (2004).

Zhou, Ping, and Jian Fang. "Intrusion Detection Model Based on Hierarchical Fuzzy Inference System." In Second International Conference on Information and Computing Science, 144-47: IEEE Computer Society Press, 2009.