Review Article **AJTL 2018,1:3**

American Journal of Transportation and Logistics
(DOI:10.28933/AJTL)

Intrusion Detection Systems Technologies and Trends

Damilola Fowora*, Oludele Awodele, Olakunle Olayinka and Oyebode Aduragbemi

Department of Computer Science, Babcock University, Nigeria

ABSTRACT

The issue of security is a major issue as regarding the use of various systems and also technologies being applied today. We live in a completely digital age and information security is paramount. Intrusion detection systems help to ensure that attacks on network systems is eradicated. This paper presents a review on Intrusion Detection Systems (IDS) details it's model and various security threats that it addresses.

Keywords: Intrusion Detection Systems, Technologies, Trends

***Correspondence to Author:**
Damilola Fowora
Department of Computer Science, Babcock University, Nigeria

How to cite this article:
Damilola Fowora, Oludele Awodele, Olakunle Olayinka and Oyebode Aduragbemi. Intrusion Detection Systems Technologies and Trends. American Journal of Transportation and Logistics, 2018,1:3.

eSciPub LLC, Houston, TX USA.
Website: http://escipub.com/

Introduction

Customarily, firewalls and access control have been the most vital parts utilized as a part of request to secure servers, hosts and PC systems. Today, intrusion detection systems (IDSs) are picking up consideration and the use of these systems is expanding. This theory covers business IDSs and the future bearing of these systems. A model and scientific categorization for IDSs and the innovations behind intrusion detection is displayed.

Today, numerous issues exist that disabled person the use of intrusion detection systems. The diminishing trust in the cautions created by IDSs is specifically identified with difficult issues like false positives. By contemplating IDS advances and breaking down meetings led with security divisions at Swedish banks, this theory recognizes the significant issues inside IDSs today.

The possibility of a framework that distinguishes intrusions in PC systems has been around for over two decades. One of the most punctual papers about intrusion detection is James P. Anderson's Computer Security Threat Monitoring and Surveillance, distributed in 1980. At to begin with, intrusion detection for t

Since trust is a sensitive temperance and frequently mishandled, an approach to secure our PC systems is to identify any malignant movement and respond to this treat as soon as it is discovered. The essential meaning of defensive acts to be carried out are stated as follows, (Dieter Gollman 1999):

he most part was an exploration subject and not something found in the business advertise. Nonetheless, over the most recent 10 years the business advertise has started to develop and the present items are getting increasingly progressed.

In spite of the fact that there has been a considerable measure of enhancements in the IDS field amid the most recent years there are some real issues left for the merchants and analysts to fathom. Subsequently, this proposal introduces the consequence of an examination with respect to IDS items and their fundamental issues today.

The possibility of a framework that recognizes intrusions in PC systems has been around for over two decades. One of the soonest papers about intrusion detection is James P. Anderson's Computer Security Threat Monitoring and Surveillance, distributed in 1980.

At in the first place, intrusion detection for the most part was an examination subject and not something found in the business advertise. Be that as it may, over the most recent 10 years the business showcase has started to develop and the present items are getting increasingly progressed. In spite of the fact that there has been a considerable measure of changes in the IDS field amid the most recent years there are some significant issues left for the merchants and scientists to comprehend.

"A protected PC framework is a framework that can be relied on to act as it is required to do" (Rebecca G. Bace 1999)

So as to accomplish this, the parts that make up the framework must, eventually, be trusted. To begin with, the equipment must be trusted to carry on not surprisingly, in this manner limiting the likelihood of equipment disappointment. Second, the product introduced and running on the framework must be trusted to act not surprisingly and third, the clients of the framework must be trusted to act of course.

Regardless of the possibility that the majority of the above is valid, everybody who could access the framework (for the situation when the PC is associated with the Internet, presumably the entire world) must be trusted to carry on of course.

1. Prevention: These are acts taken which will keep the network elements safe when attacks occur.
2. Detection: These are acts which enables network administrators to identify network elements that has been attacked, how the

attack occurred and also the cause of the attackers.

3. Reaction: These are acts that allow the network administrators to recuperate network elements that has been attacked.

Literature Review

Computer security measures can be classified in three major measures (Dieter Gollman 1999):

1. Confidentiality: Prevention of unapproved exposure of data.
2. Integrity: Prevention of unapproved change of data.
3. Availability: Prevention of unapproved withholding of data or assets.

The accompanying definition determines how intrusion detection fits in this classification of security. "Intrusion detection is the way toward recognizing and reacting to vindictive exercises focused at figuring and systems administration assets." (Edward G. Amoroso 1999)

A risk to a PC framework is characterized as any potential event, malignant or something else, that can undesirably affect the benefits and assets related with a PC framework.

Threats were broken down into 5 noteworthy security qualities which are:

1. Availability: These guarantees that the administrations gave by the system is made accessible consistently and furthermore it must have the capacity to deliver mistakes in other to have a steady association
2. Authenticity: These element of system components to approve the information sent and furthermore information got by hubs in other to make it difficult to for aggressors to access hubs and acquire delicate data.
3. Confidentiality: This includes limiting data from being spilled to unintended gatherings, simply approved clients ought to approach information.
4. Integrity: Data shouldn't be changed or modified amid transmission.
5. Non-Repudiation: These guarantees that both the sender and the beneficiary of back rubs can't deny that the trade occurred. (Geetha and Sreenath, 2016)

Threats can be arranged into the categories:

1. **External Penetration**: In this situation, the intruder isn't approved to utilize neither the PC nor any information/program assets. For instance, the intruder may be a representative of an organization who needs to get to the private intranet of an adversary organization to take client particular data from their client database. With a specific end goal to finish this, he should most likely leap forward the organization firewall and pick up root access to at least one inward servers. This intrusion is the most effortless to recognize with the present items.
2. **Internal Penetration**: In this situation, the intruder is approved to utilize the PC however isn't approved to utilize the information/program asset. For instance, the intruder could be a representative with access to the organization intranet through remote access or by his office terminal. The intruder needs to get to the organization's client documents (to which he has no entrance) keeping in mind the end goal to offer these to an adversary organization. Since he approaches the intranet it is less demanding for him to achieve this, and furthermore substantially harder to recognize, than in the case above.
3. **Misfeasance**: In this situation, the intruder is both approved to utilize the PC and the information/program asset. For instance, the intruder could be an official worker with full organization get to who wishes to pitch client data to an opponent organization. This intrusion,

when a client manhandles his benefits, is most hard to recognize. (Martin Arvidson 2003)

An Intrusion Detection System Model

Intrusion detection systems exist in a large number of configurations and there are a wide range of suppositions and assignments on what an IDS resembles. A current model, that was both finished and bland, couldn't be found. A nonexclusive model depicted in (Rebecca G. Bace 1999) was first utilized however it needed measured quality, an unmistakable stream of data and intelligently named parts. The expanded model appeared in figure beneath was created to manage these weaknesses

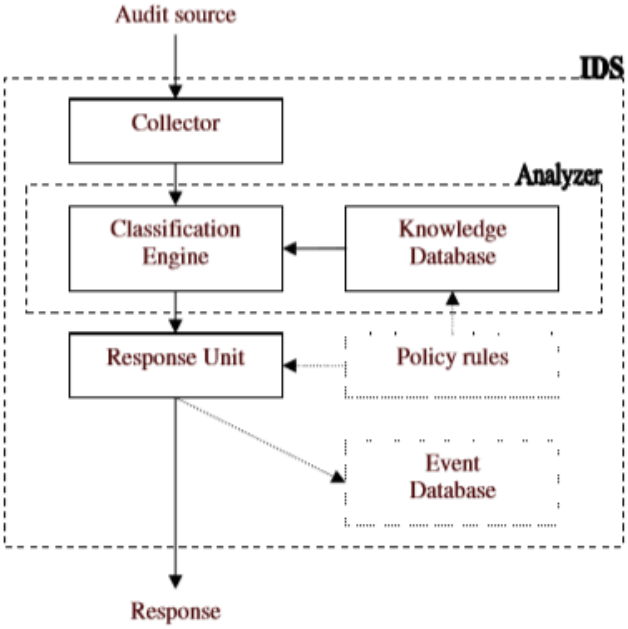

Figure 1: Intrusion Detection System Model Source: Martin Arvidson 2003

Each box is considered as a solitary part, which plays out a solitary assignment. The arrows depict the stream of data. A portion of the boxs have a lighter layout. These cases are a bit much for the IDS to be operational, albeitbut practically every IDS today uses them.

All parts can live in the same physical framework yet it is likewise workable for them to be conveyed independently. The segments are depicted in detail in the accompanying segments:

1 Collector: The gatherer tests the review source, either progressively or intermittently, and preprocesses the data. The pre-preparing incorporates change of the tested data into an inside standard arrangement, known by the analyser. A preparatory decrease of information, e.g. the gathering of comparative log passages, is regularly a piece of the pre-processing step. On the off chance that the IDS are observing some sort of association situated convention, the authority may reserve the system bundles for session recreation.

2 Analyzer: The analyser comprises of an order motor and a learning database. The capacity of the analyser is to decide whether the information sent by the gatherer contains indications of an assault. At the point when an assault is discovered, the analyser produces at least one occasions that are passed on to the reaction unit.

3 Knowledge Database: The information database is the long-haul memory of the IDS. It contains itemized assault data that shifts relying upon the kind of IDS.

4 Classification Engine: The order motor tries to decide whether the information got from the gatherer is verification of an assault. When all is said in done, it does this by contrasting the information and the data put away in the learning database as per at least one detection strategies. In the event that indications of an assault are discovered, an occasion is built containing all the applicable assault related data. The occasion is normally ordered by the seriousness of the assault and after that passed on to the reaction unit.

5 Audit Source: The review source is the contribution to the IDS, the crude information, which can have a few unique organizations relying upon the sort of IDS and where the IDS is found. Cases of review sources are application logs, IP-bundles and the yield from different IDSs.

6 Response Unit: The reaction unit chooses which activities to perform contingent upon the approaching occasions and the level of seriousness. A wide range of reactions exists.

7 Policy Rules: Policy rules enable us to design how the IDS ought to perform detection and respond to intrusions. It does this by giving us a chance to choose a subset of the learning database to use in the analyser and picking which reactions a specific occasion should trigger in the reaction unit. Since this component is discretionary, IDS without this module would dependably utilize the entire information database for intrusion detection and dependably react to assaults in a predefined way.

8 Event Database: The event database is the place all the event data delivered by the IDS is put away. The choice if an occasion ought to be logged is controlled by the strategy and it is taken in the reaction unit. The database can later be utilized as a part of a large number of ways (e.g. doing comprehensive scans or for creating reports of assault measurements).

The following are various vendors of IDS: Internet Security Systems, Cisco, Enterasys, Symantec, NFR Security, Intrusion.com, Entercept Security Technologies, Recourse Technologies

Detection Method

The detection strategy depicts how the framework identifies occasions. There are two methods for doing this; learning based or pattern based.

1 Knowledge-based: With this strategy, the framework has some sort of learning about what assaults look like. This implies everything the framework does not unequivocally perceive as an assault is viewed as typical. This is generally illuminated by utilizing marks to perceive assaults. This strategy can be extremely exact (contingent upon the mark) and in this manner, ought to have a generally low false positive rate.

2 Behaviour-based: If the detection technique is conduct based the IDS is attempting to recognize awful conduct by comprehending what ordinary conduct resembles. In the event that anything, that isn't viewed as typical is distinguished, the IDS flags that it has recognized an assault.

Behaviour on Detection

Conduct on detection, or reactions, are moves made by the IDS because of a produced occasion. The scientific classification in (Hervé Debar et al 1999) separates reactions into active or passive. Because of the presentation of intrusion prevention systems (IPSs) the dynamic classification is additionally partitioned into proactive and responsive. IPSs are intrusion detection systems that endeavour to keep an assault by utilizing proactive reactions.

1 Passive Alerting: Passive alarming manages the circulation of data. This can be actualized by sending an occasion to a comfort, paging or mailing a security

officer or whatever other activity that includes telling the fitting individual. These reactions are executed after the assault has been identified by the IDS. Inactive alarming is some of the time alluded to as aloof reaction.

2 Reactive Response: Reactive reactions change the encompassing framework condition, either in the host on which the IDS lives or outside in the encompassing system. The principle objective of these reactions is to prevent the assailant from increasing further access to assets, in this way relieving the impacts of the assault. Receptive reactions are additionally executed after the assault has been identified by the IDS.

3 Proactive Response: The main contrast amongst proactive and reactive reactions is the point at which they are executed. Proactive reactions mediate and effectively prevent an assault from occurring. A proactive reaction could be to drop a system parcel before it has achieved its goal, in this way interceding and ceasing the real assault. A receptive reaction would have possessed the capacity to end the continuous association, yet it would not have ceased the bundle that set off the IDS from achieving its goal.

officer or whatever other activity that includes telling the fitting individual. These reactions are executed after the assault has been identified by the IDS. Inactive alarming is some of the time alluded to as aloof reaction.

2. Reactive Response: Reactive reactions change the encompassing framework condition, either in the host on which the IDS lives or outside in the encompassing system. The principle objective of these reactions is to prevent the assailant from increasing further access to assets, in this way relieving the impacts of the assault. Receptive reactions are additionally executed after the assault has been identified by the IDS.

3. Proactive Response: The main contrast amongst proactive and reactive reactions is the point at which they are executed. Proactive reactions mediate and effectively prevent an assault from occurring. A proactive reaction could be to drop a system parcel before it has achieved its goal, in this way interceding and ceasing the real assault. A receptive reaction would have possessed the capacity to end the continuous association, yet it would not have ceased the bundle that set off the IDS from achieving its goal.

Problems and Challenges

Conduct on detection, or reactions, are moves made by the IDS because of a produced occasion. The scientific classification in (Hervé Debar et al 1999) separates reactions into active or passive. Because of the presentation of intrusion prevention systems (IPSs) the dynamic classification is additionally partitioned into proactive and responsive. IPSs are intrusion detection systems that endeavor to keep an assault by utilizing proactive reactions.

1. Passive Alerting: Passive alarming manages the circulation of data. This can be actualized by sending an occasion to a comfort, paging or mailing a security

Applications of IDS Today

Almost all of the banks use some kind of IDS today, though the usage of the system varies a lot. The majority use a commercial product but in-house developed IDSs were also seen. The use of IDSs is relatively new in most of the banks although one bank has actually had some kind of IDS for almost six years.

The one bank that did not use an IDS had performed intrusion tests in collaboration with an external contractor, with an IDS up and running during a two months period. The tests showed that the IDS did not offer any additional security over the other systems.

All of the banks that use IDS, except one, have the system maintained by their own employees. The one that has outsourced their IDS is looking for ways to implement a system that is operated by their own staff instead

. The banks that use IDS treat it as a separate system. It does not communicate, in any way, with other systems (e.g. firewalls and vulnerability scanners). Some has continuous monitoring of the system and some only look at statistics and log files in the case of an incident. The configuration of the systems also varies a lot. In some cases, the security department wants to see everything that goes on in the network, and thereby they have quite a lot of alarms and false alarms.

The reason for this is that the main use of the IDS is to log whatever happens and with this log create statistics of the traffic flow and the attack patterns. Others have a very strict configuration, where they only see the most important events. Therefore, they do not have a big problem with false alarms. The banks that implement this strict configuration also have higher confidence in the IDS and the alerts it generates.

None of the banks see the ongoing maintenance of the systems as a large problem, but the installation and initial configuration was a lot of work. As long as there are no big changes in the network architecture, the only real work, except for handling alarms, was to keep the system updated. This was not a problem for any of the banks.

All of the banks were using some kind of statistical, regularly generated, report from the system, or were soon about to implement this. These reports were one of the main advantages of the system since they give a lot of information about traffic flow, misconfigurations in the network and attack patterns. None of the banks that had implemented an IDS were dissatisfied with the system. They all thought it was a good complement to their other security systems.

Conclusion

Today, most of the banks use some kind of IDS in their network. The use of the system varies but none of the banks use automated responses and all of them have problems with the confidence in the events that are generated. The IDSs today are only a complement to existing security solutions, but the usage of IDSs and the investment in these systems will rise in the near future. The overall image that the banks gave during these interviews is mainly positive; the IDSs provide increased security for their networks.

References

1. Aarti, & Tyagi, S. S. (2013). Study of MANET: Characteristics, Challenges, Application and Security Attacks . International Journal of Advanced Research in Computer Science and Software Engineering .
2. Alkharashi, A. (2016). Wireless & Telecommunication. 2nd International Conference and Business Expo . Saudi Arabia: Open Access Jorunal.
3. Faisal Shahzad1, M. F., Ullah, S., Siddique, M. A., Khurram, S., & Saher, N. (2015). Im-proving Queuing System Throughput Using Distributed Mean Value Analysis to Con-trol Network Congestion. International Journal Communication, Network and System Sciences.
4. ICE. (2016). What is Simplex, Half-Duplex, Full-Duplex. Retrieved from ICE: http://www.iec-usa.com/Browse05/DTHFDUP.html
5. Mangrulkar, N. S., Patil, A. R., & Pande, A. S. (2014). Network Attacks and Their Detec-tion Mechanisms: A Review . International Journal of Computer Applications .
6. Mohamed, Sahib, S., Suryana, N., & Hussin., B. (2016). Understanding Network Con-gestion Effects On Performance. Journal of Theoretical and Applied Information Tech-nology.
7. R.Ragupathy, & Sharma, R. (2014). Detecting Denial of Service Attacks by Analysing Network Traffic in Wireless Networks . International Journal of Grid Distribution Compu-ting .
8. Raja, L., & Baboo, S. S. (2014). An Overview of MANET: Applications, Attacks and Challenges. International Journal of Computer Science and Mobile Computing .
9. Scheme, S. o. (2015). Noureldien A. Noureldien; Saeed K. Saeed; M. Ahmed Salih; Al-sawi M. Ahmed. British Journal of Mathematics & Computer Science .
10. Singh, M., & Kaur, G. (2013). A Surveys of Attacks in MANET. International Journal of Advanced

Research in Computer Science and Software Engineering .

11. Sugeng, W., Istiyanto, J. E., Mustofa, K., & Ashari, A. (2015). The Impact of QoS Changes towards Network Performance. International Journal of Computer Networks and Communications Security .
12. Sutton, A., & Tafazolli, R. (2015). The Future of Mobile Communications. ITP Journal Insight.
13. Zanoon, N., Albdour, N., Hamatta, H. S., & Al-Tarawneh, R. (2015). SECURITY CHAL-LENGES AS A FACTOR AFFECTING THE SECURITY OF MANET: ATTACKS, AND SECURITY SOLUTIONS . International Journal of Network Security & Its Applications .