INTRUSION DETECTION SYSTEMS – A LEGACY FROM SECURITY PERSPECTIVE IN ALL SORTS OF NETWORK COMPUTING

Abstract

The Intrusion Detection System (IDS) is intended to be a software program that serves as a security system and protective layer for the infrastructure. It also keeps an eye on the network and detects any suspicious activity. Internet usage is increasing at an exponential rate, which raises questions regarding how to safeguard digital information. The IDS technology has advanced significantly over time to keep up with the growth of computer crime. Hackers today employ a variety of techniques to access our computers' personal, secure data. Numerous intrusion detection approaches, tactics, and algorithms will serve as a defense against these threats.

Despite the researchers' tremendous efforts, IDS still has difficulties detecting fresh intrusions and improving detection accuracy while lowering false alarm rates.

Keywords: Intrusion Detection, Botnets, HIDS, NIDS, IPS, Intrusion Security.

Authors

Sanjiw Kumar
Assistant Professor
Department of Computer Applications
Information technology
A. M. College, Gaya
sanjiwkr@gmail.com

Malay Kumar
Assistant Professor
Department of Computer Applications/
Information technology
A. M. College, Gaya
malykumar@gmail.com

I. INTRODUCTION

The current state of affairs in the field of information security reveals an alarming rise in the frequency and severity of assaults. Automated attack tools improve the volume and velocity of attacks while simultaneously reducing the amount of information needed to breach security and simultaneously increasing the complexity of the work required of security professionals. All businesses now must have access to the internet. Information networks, data storage systems, different encryption methods, Voice over IP (VoIP), remote, wireless access, and online services are just some of the ways that government agencies and enterprises have adapted to the needs of modern business. Virtual private networks (VPNs) have become increasingly popular among employees for gaining unauthorized access to workplace networks, and this has contributed to increased network congestion.

The rise in popularity of extranets as a means for business partners to share information and collaborate, as well as the prevalence of e-commerce and CRM-enabled customer-company partnerships(CRM). The network of major companies and government institutions has been compromised. Network damage is increasingly easier for attackers to do, and attacks are more sophisticated than ever. As F. pointed out, as the number of networks grows, so too do the number of attempts to breach them. Gong (2002). So, nowadays, disgruntled workers, dishonest businesses, and even terrorist organizations all utilize the internet as a communication channel to spread false rumors, steal trade secrets, and cause economic, social, and political chaos (confusion).

According to studies conducted by the Computer Investigations Unit (CSI) and the Federal Bureau of Investigation (FBI) in 2010, hacking and malware are the most common forms of assault. Eighty percent of 2010's data loss was traced back to malware, of which about half occurred in the first half of the year. Examples of malware with data-exfiltration, backdoor, and key logger capabilities were located in the caseload, and they are all illustrated on the website Gocsi.com (2007). Fragile or stolen keys are the bane of corporate security. There is a problem in the financial service, trade, and industry sectors due to the use of default keys throughout the course of operations. Supporting evidence may be found in F. Wu' s 2011 assessment on the security of the aid network. According to Gong (2002), intrusion detection approaches, including as signature detection and anomaly detection, are necessary to strongly secure industry and government networks from the whole spectrum of threats. The IDS should be able to accurately identify intrusions and safeguard the integrity of the network' s data. As a result of their imprecise performance and flawed detection mechanisms, IDS devices are often not even deployed. F. This illusory sense of security provided by Gong (2002) is useless when actual threats materialize. Therefore, it is necessary to create and distribute an appropriate solution to help companies and governments safeguard their networks against intruders. Lu, Nannan, et al., have stated the benefits of data mining techniques and sentiment analysis in the field of intrusion detection systems; this study aims to research and build such a creative solution (2013). Before going towards an efficient intrusion detection system this chapter emphasizes the numerous introductory fundamental principles which are associated with intrusion detection field.

II. INTRUSION DETECTION SYSTEMS: BASIC CONCEPTS

This section illustrates the basic concepts related to intrusion detection with all details of functionalities. The details of IPS are given to understand its working phenomenon in subsequent section.

1. **Intrusion, intruder and intrusion detection:** Ankit Fadia (2011) specified that Intrusion Detection system is surrounded by many security techniques which are designed to detect and report harm system and network activity or record the proof of intrusion detection system. One has to understand what *intrusion* is to get details on intrusion detection. Abeer Saif (2006) defined the definition of intrusion and same can also found in S.A. Joshi and Varsha S.Pimprale (2013). An intrusion is firstly illustrated by Anderson (1980) and its definition is available in Security Glossary (2011)**.** Intrusion could be an instance of a legitimate user trying to escalate his privileges so that he can get greater access to the system. Hack This (2014) presented that he is at present assigned, or a lawful user trying to connect to a remote port of server to which he is not authorized, or a remote or unauthenticated user trying to compromise running service in order to damage the resources and data. Intrusions can be generated from the outside world and discontented member of staff. Even from your own trusted staff. Intrusions are categorized into following classes as given in Junqi Wu (2008).Misuse intrusion are well defined attack which are done on weak passwords within a system .This is detected by examine the proper actions which is suitable and performed on the particular object. Anomaly intrusions are based on observations of deviations from normal system patterns. Diego Zamboni (1999) specified that anomaly (irregularity) detections are usually detected by creating profile of the system and significant deviations in profile as defined in Mark Merkow (2000). Kottu (2014) defined, an *intruder* (also known as an *attacker*) is the first element in the attack model of intrusion. An intruder is a person who attempts to gain the illegal admittance to a system, to break that system, or to concern data on particular system. He or she tries to infringe the safety and recovering proper error by compromising the availability, data integrity and confidentiality of system as given by Hitachi ID (2001). The term *Intrusion detection* includes various methods like detection of intrusions, generating alerts, reporting intrusions, correlating with systems, security actions. Intrusion detection is mainly used for identifying the events, actions occurred in computer system, computer networks and are studied to identify realization of intrusion as specified by SANS Institute (2001), Abeer Saif (2006) and Divya, Vikram Nandal (2014).

2. **What is an IDS?:** IDSs are mainly used to detect intruders as stated by Nallagorla Vijaya Gopal Ardhala Koteswaramma (2013). It is a software and or hardware that monitor the traffic for unauthorized and or unwanted access to computer systems and networks. Firewalls and other security measure that works to discontinue intruders, IDS detects intruders that are accessing the network or those that are already in the network. At the same time, the regular security measures detect activity from outside source whereas IDS detects both internal and external attacks. IDS can be either passive or reactive. Out of this, passive systems are used to detect intrusion activities, to generate logs and account to the administrators. It does not take any action. It is up to the administrators to determine the type of response that should take place to resolve the problem. On other side, reactive systems are more usually recognized as intrusion prevention systems. These systems take

step by resetting the network connection or blocking the network intruder with automatic provision or by an operator. The selection of system relies on the requirements of the business.

3. **Types of IDS:** There are several ways to categorize the types of IDS that are available. Depending on the kind of activities, transactions, traffics or systems they observe. IDS can be classified as Network based (NIDS), Host based (HIDS) and Application based (APIDS). Based on differing approach to episode investigation, IDS can be classified between Signature based (SIDS) and Anomaly based. Each type of IDS has its own strengths and weaknesses are also illustrated.

    - **Host based IDS (HIDS):** HIDS monitors incoming and outgoing activity on a particular system in the network. It monitors the dynamic behavior and state of the computer system. The manager will be informing once an infringement has been detected. In this case, NIDS is usually used alongside a HIDS to identify any activities that HIDS overlooked.

    - **Network based IDS (NIDS):** NIDS monitors the incoming and outgoing network traffic to identify intruders. Intruder access the network through hubs or network taps and look for suspicious patterns by reading incoming network packets. In addition, they also scan outgoing traffic for the possibility of an internal intruder. The fact that Intrusion detection in incoming as well as in outgoing traffic is identified and NIDS are placed within the network. Due to NIDS it slows down overall speed of network.

    - **Hybrid intrusion detection system:** This combines both features of host based IDS and network based IDS. It is used to monitor the network. In this, Host-based IDS is used to monitor events occurring at the host level and Network-based IDS is mainly used to monitor the network related activities.

    - **Application protocol based IDS (APIDS):** Application Based IDS monitors activity in the specific protocols used in the computer system. It inspects for protocols and emphasizes the correct use in the systems.

    - **Signature-based IDS (SIDS):** SIDS works in the same way most anti-virus software performs. Anti-virus software monitors the network for activities that **have** been predetermined to be malicious. New threats will not be detected by SIDS as like anti-virus software. Hence there will be difference between time when new threat are discovered and the time SIDS actually detects it on the network.

    - **Anomaly-based IDS:** In anomaly-based IDS, a performance baseline is established to reflect what a normal network activity should be. Network traffic is sampled and compared to the baseline to determine whether the action is usual. It cannot be guaranteed that intruders cannot tamper with the systems. The most dominant weaknesses are the difference in time to update and the speed reduction due to the monitoring of traffic inside the systems specified by Sharada K A *et al.* (2012) and found that the high false alarm rate is also a major concern with these IDSs.

4. **What is an IPS ?:** Almost all corporate networks (including personal systems) are protected by firewalls. However, S.A. Joshi and Varsha S. Pimprale (2013) specified that these firewalls are not always effective against the emerging intrusion attempts. Firewalls used in networks and in desktop or laptop machines are used to control traffic from private network. Also, it is a good solution for hardware and software to enforce a security policy over private network. These are not always available to detect intrusion because they are depending on list of permit and deny rules. Even, firewalls are unable to provide protection against malicious codes, inside attack. It will only be successful as one of the available lines of defense. The shortcomings in the current security systems have driven the requirement of new security solutions known as Intrusion Prevention Systems. IPSs are considered as security mechanisms intended to protect against network intrusion penetration, blocking the unauthorized traffic automatically before it does any damage for computer systems and resources. As given on Wikipedia page of Intrusion prevention system (2010)**,** Level of security is provided by firewall as user authentication, data encryption and virtual private network but this is all intrusion prevention system. Also, it is considered as extension of intrusion detection system because this both monitor network traffic or system activities. The alternatives found as stated by Robert C. Newman (2009) and Michael E. Whitman; Herbert J. Mattord (2009), intrusion prevention systems are capable to detect, prevent intrusions that are detected in earlier stage. In Intrusion prevention system (2010), IPS can take preventive actions as stated by

   Tim Boyles (2010). Intrusion prevention systems can be classified as

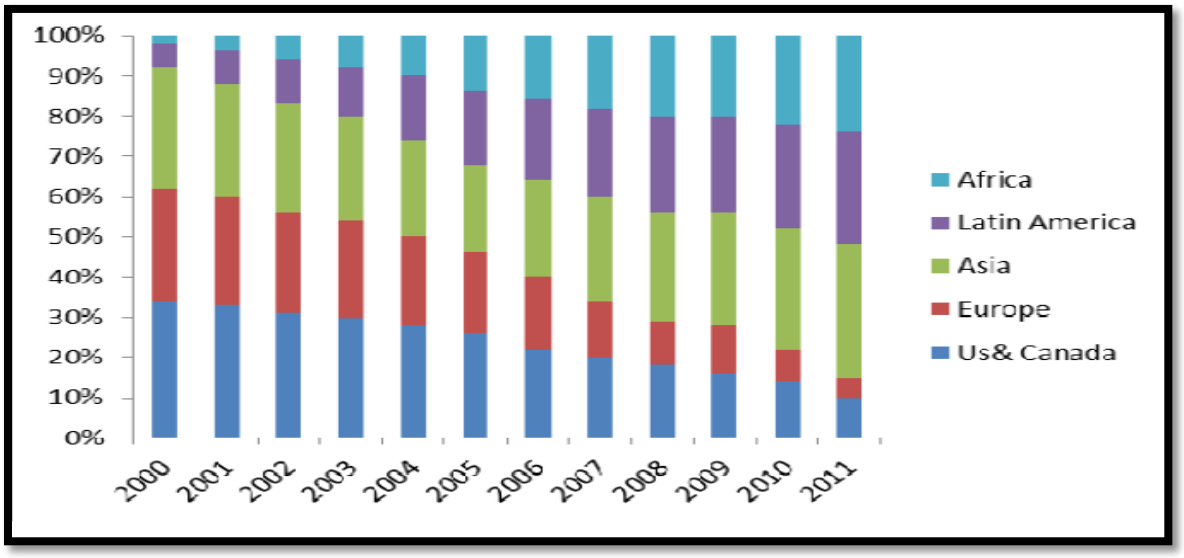
   - **Network based Intrusion Prevention:** It monitors entire network for un-trusted traffic by analyzing protocol activity.
   - **Wireless Intrusion Prevention System (WIPS):** WIPS is used to monitor the wireless network traffic by analyzing wireless networking protocols.
   - **Network Behavior Analysis (NBA):** It is used to identify threats that generate unnecessary traffic flow such as DDoS are type of malware as well as policy violation.
   - **Host based Intrusion Prevention (HIPS):** HIPS is software package used to monitor single host for suspicious (untrusted) activity by analyzing events occurring within host.

5. **Why Should We Go In For An IDS And Or IPS?:** The initial development of IDS was aimed at protecting the network and its vital information from the outside world. However, this is now changed as more and more organizations including government agencies want to monitor their internal networks because the study shows that major losses in the commercial sector involve insiders. Therefore, corporate enterprises want to use the IDS in any of the following combinations: To track down insiders, catch them in act, get the evidences required for penetrations, and protect vital information resources before their damages and stealing. The major concern of deploying IDS is, technology is still in its infancy and intrusions are getting missed because of its immature usage. Additionally, new attacks are emerging very rapidly and coming out at each month and the IDS technology must adopt these rapid changes and provide security at its optimum level. Following are the reasons for using IDS and IPS technology over the traditional network management and system monitoring tools:

- Provide worthwhile information about malicious traffic.
- Greater proficiency in detecting intrusions rather than by doing it manually.
- Help to identify the sources of incoming intrusions or attacks.
- Able to sustain with large volumes of data.
- Real-time detection by IDS and alerting capabilities by IPS.
- Automatic responses for detected intrusions.
- Built-in reporting capabilities.
- Forensic evidences can be collected, which could be used to identify intruders.
- IDS and IPS help in quantifying the attacks against the network.
- IDS and IPS assist in establishing an overall defense-in-depth security strategy.

III. GROWTH OF INTERNET AND INTERNET ATTACKS

At late seventies the internet came into world as an outcome of ARPANET. DoD project has grown very fast due to existence of internet by Ciza Thomas (2009). (IT Law.wikia.com) described Internet has changed in three important ways over the past decade: content has advanced from relatively static text and web pages to multimedia high-bandwidth content that requires low latency; usage has rapidly globalized; and access has moved beyond desktop computers using fixed connections to a variety of new devices using mobile broadband. Prominently, the speed of this evolution in technology and its acceptance is supreme in human history. Analysis Mason (2011) brought out, at the same time that services are growing, the Internet is globalizing at a hastening speed. Figure 1 shows how Internet access has moved from being centered on the developed world in 2000, to becoming more and more attentive on developing countries by 2011, more with the world population as specified by Analysis Mason (2011). Most needed and useful device none other but internet which has given a worldwide or globalized dimension to the world quoted in Ciza Thomas (2009). It is the widespread source of information.



[Source: ITU, Analysis Mason (2011)]

Figure 1: Geographic Distributions of Internet Users

Over the past decade, the number of Internet users in Africa has increased at an annual rate of 33%, which is about twice as fast as the rate in Asia and Latin America (both at 17%) and far ahead of the growth rates in Europe (10%) and the United States and Canada (both at 2%). (4 percent). Large- scale shifts have already place, with much more needing to be done. This is especially true with regards to expanding access to broadband (on both fixed and mobile networks) in developing nations. According to Ciza Thomas (2009) , the expansion of the internet after the seventies occurred at a breakneck pace, bestowing onto contemporary society a plethora of useful and exciting new capabilities. The proliferation of internet access and use poses a significant security risk. Increased internet usage has led to a rise in cybercrime in recent years. The proliferation of online resources has coincided with a rise in harmful assaults. In this way, with the proliferation of user-friendly platforms and a generally more conducive ecosystem, cyber attacks have become trivial. A network intrusion may happen in a number of different ways; for example, an IP packet might crash a target host, and software system security concerns have spread to every type of network, from legacy systems to decentralized ones. Operating system frequently broadcast the update, however owing to growth in threats, the operating system and organization are handled incorrectly.

1. **Cyber attacks:** Cyber-attacks are primary point of digital assaults will be to erase, take or alter the data on target machine framework. Vatis (2002) found groups distinctive sorts of digital assaults as:

    - **Unlawful interruption:** in which aggressors utilizes diverse hacking systems to enter into framework. In case of organization, the insider goes through his approved access and break organization system for some reliable data.
    - **Viruses or worms:** These are get abused from one machine to an alternate in different structures such as messages.
    - **Denial of administration assaults:** Lead to system burglary with unimaginable movement load.

    Few politically motivated attacks that are prevalent today, the details excerpted from Purvag.com (2011) are given below:

2. **Changing the web page content and increase in false information:** This is done by web defacements and semantic attacks. In today's network the domain name server attacks are used. In this, when user request a particular website because of wrong IP address generated by DNS server. Distributed denial of service attacks has communication at high rate towards targeted computer, where cyber attackers focus on the target machine to slow down this system. These communications are taken from web servers and email servers and diverted to target computer to create blockage and ultimately slow down or shut down machine. Types of malicious code as per classification are viruses, worms, and Trojan horses. The system administrators are well aware of viruses and worms that can be caught and recover, but there are certain malicious codes that are easily looked into system administrator which is detected only after deleting information.

3. **The routing disarrays lead to attacks which may** destroy the internet also the concept of compound attacks occurs which says that attackers can combine number of attacks and make sequence out of them which can end everything and has no possibility to recover it. Hence, laws are made to monitor such attacks, but these laws are not use for business to recover or get back on same track as it was before. Etsebth (2011) argued that businesses should not only protect their information but should be confident of whom to give access to information. Cyber attackers are classified in three ways:

    - **Intervention with information and / or data:** This occurs when availability, confidentiality and integrity of the information are compromised by challenger.

    - **Interruption of information and / or data:** It modifies or deletes compromised data.

    - **Masquerade:** It should be an authorized individual. It also states that information security is required to be done because it tends to threaten the information assets of business which directly shows performance and efficiency of business. One of latest attacks was on Twitter Account of fox news by cyber hackers. They call themselves as Antisec. This hacker group reported that president Obama was shot dead. Although, there are no economic consequences in this particular case, but this information is exist with different websites that hold extremely important and sensitive information. Such attacks can lead to monetary losses, though they are simply hoax. Focusing on India, e-commerce is become more prevalent since the last decade. A key finding of the Economic Crime Survey (2006) was that a typical offender of economic crime in India was male (almost100%), a graduate or undergraduate and 31-50 years of age. Further, one third of the frauds were from insiders and over 37% of them were in senior managerial positions.

    Trying to identify how widespread is the crime in India and across the world, it is found that very few cases of cybercrime occurrences are actually reported across the world. In India, cybercrime cases recorded are less compared to the US, Europe, etc. The Internet Crime Complaint Center (IC3) 2006 ranks the US (60.9%) as first among the nations in hosting perpetrators followed by the UK (15.9%). Many countries, including India, have established Computer Emergency Response Teams (CERTs) with an objective to coordinate and respond during major security incidents or events. These organizations identify and address existing and potential threats and vulnerabilities in the system and coordinate with users, stakeholders to address these intimidations.

4. **Concerns related with attacks:** According to Analysis Mason, Purvag.com (2013) emphasized the many ways in which the monetary costs associated with cyberattacks can vary depending on the level of analysis performed (2013). The United States invests a lot of money and time on its military to ensure their safety. Due to the same severity of the risks involved, substantial resources are expended to increase cyber security. Republic of China planned to attack the infrastructure of American businesses and government agencies. Accordingly, the PRC has nurtured hacker organizations capable of developing logic bombs and dispersing them throughout international computer networks. The main target was the federal network in the United States, but they also aimed against other

networks across the globe. According to the Cyber Attacks Statistics Summary (2013)and Analysis Mason(2011), Chinese enterprises have sold Cisco routers and servers to a large number of western customers after reverse engineering them. To slow down or otherwise flag their cryptographic systems, the Marines, the Air Force, and other defense contractors. Instead of investing heavily in weaponry and heavy industry, China has prioritized the information technology (IT) sector in the sphere of security. To protect corporate and government networks, cyber squadron personnel should be provided with every available resource, including a rock-solid supporting infrastructure. Cyber attacks have more economic repercussions.

According to Analysis Mason (2011) and Purvag.com (2011), Google Inc. discovered a Chinese-origin assault in 2010. This is only one example of how privacy is effectively nonexistent in the modern world. Spear phishing was employed in this attack to get access to the Gmail accounts of Chinese dissidents. As a result, stringent security measures have been adopted with the goal of preserving the existing underpinnings and preserving an adequate level of protection. During this time, they realize that installing infrastructure via using fiber optic cable, routers, and servers through ISPs is not sufficient and poses a significant challenge. Since 1982, the United States has also been a target of cyber attacks. It follows that American officials are similarly making weighty prognostications under assault, while having few data and a very short window of opportunity in which to act. Mason (2011) compiles worldwide statistics characterizing the InfoSec scene in 2012 and makes appeals based on data from 2013. Since the dates (from which the statistics are derived) are publicly available, the data can only indicate cyberattacks that were exposed and got global attention in the press, hence the charts should not be seen as a complete picture of the threat landscape.

Before diving into the details of the most recent year's data, Cyber Attacks Statistics Summary (2013) suggests taking a look at the trend over the previous three years (with the caveat that data for 2011 is incomplete as given in Analysis Mason (2011), as it was consolidated into a form equivalent with year 2012 and year 2013 only starting in September). After an initial peak, the line for 2013 shows a progressive reduction, as stated and concluded by Analysis Mason (2011) reaching a steady state, as seen in Cyber Attacks Statistics Summary (2013). This may be because, as shown in Figure1.2, the impact of attacks inspired by hacking activities is relatively small over the course of a year. Historically, hacktivism has been most common at the start of the year. There is no much of a seasonal pattern to cybercrime; it peaks in the second part of the year. This trend does not indicate a decrease in hacktivism, but rather that its meaning shifts seasonally. Local events have gradually replaced global activities carried out by the unknown (for instance, the cyber-attacks in India and Pakistan). DDoS assaults on U.S. banks can also be felt strongly in January and February.

IV. NEED FOR INTRUSION DETECTION SYSTEM

Ciza Thomas(2009) studied, Intrusive attacks are known as network attacks too which includes attacks like services and the various attacks like data driven attacks on applications, host based attacks like privilege escalation, unauthorized logins and access to sensitive files, or malware like viruses, worms and Trojan horses. These various intrusions try to achieve the integrity, confidentiality or availability of a resource. It produces into denial of service,

system unresponsiveness, and data loss or data damages. Jaydip Sen (2010) described earlier, the unauthorized use of a system or attacks on a system or enterprises networks detection is being performed by Intrusion detection. In order to detect intrusions as concluded by Vangie Beal (2005) an Intrusion Detection Systems (IDS) which is in one of the form viz; software or hardware.

CERT-In (2003) indicates organizations are improved and they are coming with vast organizing network and are dependent on information systems. So, to protect their systems from the threats Intrusion Detection System is necessary.

It is common practice for IDS to function in tandem with a network firewall. It is a frequent misconception that, as Junqi Wu (2008) put it, modern firewalls can automatically identify and prevent intrusion attempts. According to a paper from the National Defense University Carol I (2010), firewalls serve as network gateways, but only for a chosen few. Aside from being unable to tell whether or not a person trying to enter via the gate is permitted, it lacks the capacity to identify a complete stop. Access to the designated network nodes is denied by the firewall. Security cameras, motion detectors, and burglar alarms can tell you whether or not unauthorized people are coming through authorized entrances and whether or not confidential information is being extracted. Since the IDS proposed by the SANS Institute (2001) may be set up to react to such activities, IDSs are utilized as the additional level of protection alongside the firewall in any protected network against attacks that undermine the security actions, as Junqi Wu (2008) also concluded. The need for Intrusion Detection Systems (IDS) once a firewall has been installed has been called into doubt. To do so successfully, one must be familiar with both firewall and IDS and their respective benefits and drawbacks. The importance of firewalls and IDSs in protecting networks and data will be highlighted. Firewalls and other old methods of network security, as examined by Ciza Thomas (2009), were shown to be inadequate against modern threats such as Denial of Service and Distributed Denial of Service assaults, worms, viruses, and Trojan horses. Not even this could keep up with the ever- increasing frequency of Internet threats, which highlights the need for IDS in modern network and Internet security architectures.

The Internet's reach spans many regions. As a result of the widespread nature of internet usage today, several forms of online fraud are commonplace. Both malicious outsiders and dishonest insiders, such personnel looking for payback or personal benefit, are responsible for these schemes. This fraudster group is operating on the inside, where their actions cannot be detected by firewalls. Packet filtering firewalls often examine a packet's layer 3 and layer 4 protocol information to determine whether or not it should be allowed into or out of the internal network. According to Joe Bowling's (2003) research, firewalls seldom change.

Based on research by Obbo Aggrey (2007), a firewall is any hardware or software solution that compels users to adhere to a predefined set of rules on acceptable behavior within an internal network. Access to and egress from a private network can be restricted using firewalls. Firewalls, then, are merely lists of allow and deny rules that can' t possibly detect any more infiltration attempts.

E. E. Ogheneovo and B. R. Japheth. Firewalls, user authentication, data encryption, and virtual private networks (VPN) all contribute to a higher degree of security, but they aren & #39; t impenetrable to all threats; for example, malicious software, inside assaults, and insecure modems. Accordingly, these are only useful for defense in one of the aforementioned ways. This means that they would only be effective as one of the available barriers. In 1980, Anderson introduced the IDS for the first time, and it was formally presented or put out by D.E., as Obbo Aggrey (2007) also explained. Denning in 1987, and since then it has gone on to attain phenomenal success.

According to the argument made by R K Sharma et al. (2013), IDSs can identify malicious activity and offer comprehensive data on the dangers that exist. Those actions, as stated by Obbo Aggrey (2007), are visible via the network when normal security measures are circumvented. Even when firewalls are put in place to prevent malicious data from passing across the network and to halt all connection, intrusion detection systems are still required. Internal assaults cannot be detected by firewalls. Firewall operates at the edge of the network and may simply be responsible for regulating inbound and outbound data flows. That means a huge number of prospective hackers already inside the network will be let free.

Some of the reasons therefore for using IDS as reported by Obbo Aggrey (2007):

1. To perform twofold check incorrectly arranged firewalls. The objective of security experts is to give items that will both moderate interruptions while in the meantime permitting access to vital system administrations. Therefore other than giving a reasonable methodology to system security like other interruption avoidance components, IDS's will help system experts with included gimmicks that won't accommodate interruption location additionally give more system administration capacities.

2. To get assaults that firewalls illegitimately permits through, for instance the assaults on web servers. It is basic that when frameworks are subverted, the executive is alarmed. Interruption location frameworks will do this by sending alerts or sends to a support.

3. IDSs additionally through their logs permit getting of fizzled endeavors.

4. Gets inside assaults. A portion of the greatest dangers to any corporate system are its own particular inward clients arranged inside the system border since firewalls that are generally being utilized, are conveyed on the system edge. But assaults beginning from inside the system can result into genuine lawful troubles or even Internet integration. IDS's can screen both interior and outer assaults.

5. For quite a while system instruments have been costly and free apparatuses were practically selective to UNIX or Linux frameworks. However, this is no more the case with the approach of Nmap for windows. The expansion of the GUI interfaces as a gimmick on most open source applications, for example, grunt has further changed this perspective. Therefore, it is no more as immoderate to get them.

6. The information obtained from the IDS can be used as an evidence or proof against the criminals and will help the crime branch officers in tracing them. This information also helps in analyzing the threats or the

7. Vulnerability of a network.

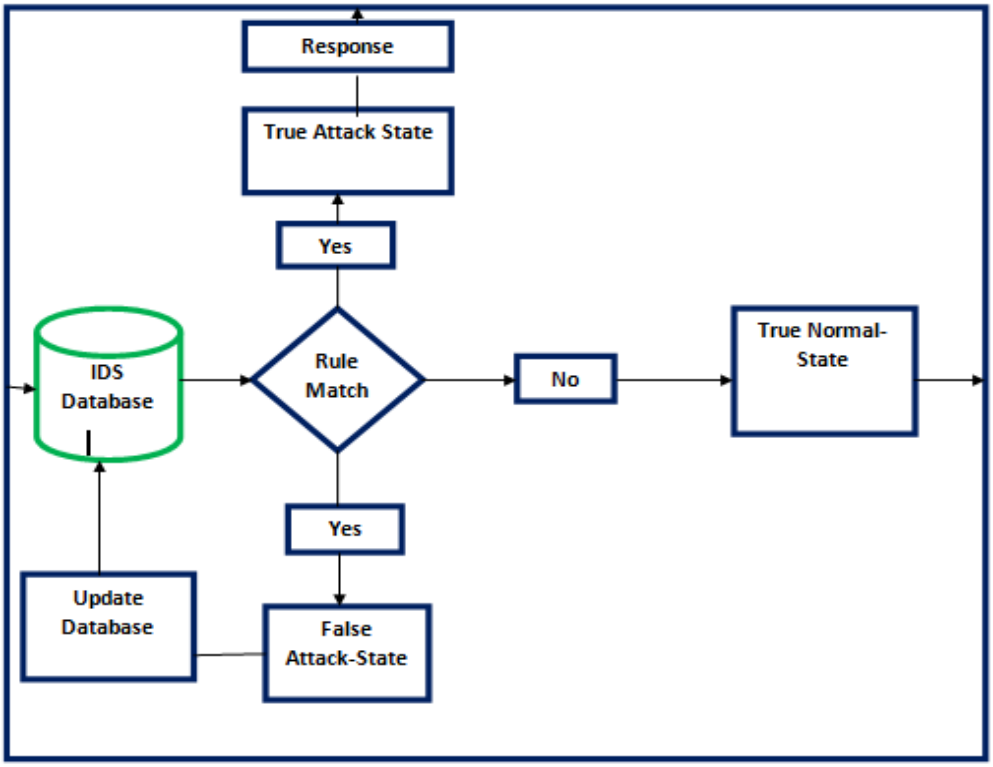


Figure 2: Classical Misuse based Intrusion Detection Model

Junqi Wu (2008): Alexis Cort (2004) and Junqi Wu (2008) concluded a commonplace abnormality recognition model known as anomaly dependent model investigates data, compare to a known ordinary profile, run factual examination to figure out whether any deviation is noteworthy, and alarms the event(s) as a True Attack State, False Assault State or Normal State. On the off chance that it discovers a false positive, the profile must be redesigned to reflect the results.

Junqi Wu (2008) also illustrated as the model ignores the probability of a False Negative, such that the framework does not get an interruption; the suspicion made here is that the IDS is setup in a ―all movement is conceivably vulnerable express, that the edge qualities are situated sufficiently low (to permit the activating of false positives amid the learning procedure), and that the gatecrasher has not bargained passwords or other approved method for getting access.

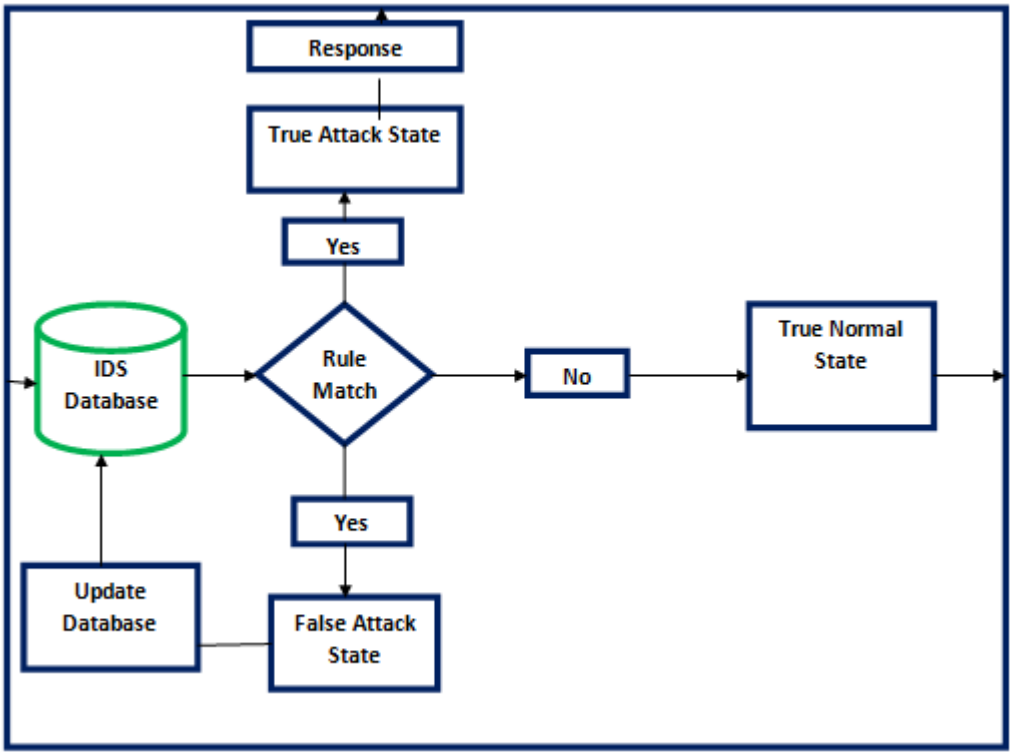


Figure 3: Classical Anomaly based Intrusion Detection Model

1. **Current IDS Theory, Challenges, and Limitations:** These days, users may take use of very sophisticated cyber security solutions that are widely available on information networks like the Internet. Additionally, the extent of vulnerabilities or incursions is also raised possibly at the same time. Security must be regarded the primary issue and research component of an organizational information network and communication infrastructure, and it makes sense that one can no longer rely on such advanced security methods for personal safety.

   The significant study and research is done on IDS over the last few decades, However, it is still has major issues to tackle in the field of information security as found in Alserhani, Faeiz(Awan, Irfan U. and Cullen, Andrea J.)(2012). Data analysis procedure for intrusion detection is always slower and requires extensive computational time in most of the IDS. Mainly, IDS executes their detection procedure to detect intrusions, once the intrusions have occurred. There is still no IDS is capable to catch the intrusions during its entry into the information infrastructure and in its running state.

   According to F.Gong (2002), hackers have affected the networks of well-known brands or government agencies, and the well-trodden information network paths of these organizations render them weaker than they have ever been. Criminal activity in the digital realm is also no longer the exclusive domain of lone hackers or unmotivated aggressors. Terrorist groups, dishonest businesses, and disgruntled workers all use the internet to get access to sensitive data, do financial damage, and create unrest among the general populace. It's hardly surprising that network attacks are on the rise, as seen in F, given that networks are weakening and hackers are ready to wreak havoc. Gong

(2002). Further, several security concerns have contributed to a general lack of information about or understanding of the incursion activity. These challenges are why organizations like the Computer Investigative and

Forensics Center (CSI), the Federal Bureau of Investigation (FBI), and the Computer Emergency Readiness Team (CERT) are essential for keeping tabs on the latest Internet security threats and incursions. False positives, in this other world, are one of the most significant challenges when using IDS. When comparing the frequency of assaults to that of normal activity, a large number of false alarms might be used as an indicator of how well IDSs are functioning. Alert log files from the user terminals, firewalls, routers, networks, etc. utilized by the company's information network are notoriously difficult to collate. Another major difficulty is that intrusion detection system (IDS) alerts need to be monitored and evaluated by IDS experts.

Different commercial and open source IDS are created and explored during the last two decades based on intrusion detection models. In this way, the efficacy of various IDS types depends on the specific safeguards put in place to identify those intrusions. We see that the outcomes vary, which points to the need for effective IDS that can identify a variety of intrusions. This is a strong indicator that there is still room for improvement in IDS and that more cutting-edge implementation solutions are needed.

2. **IDS related Issues that need to be addressed by IDS:** Although there has been extensive study of IDS, the following are some of the most pressing problems that have yet to be solved by existing technologies: Regardless of our choices in terms of supply or network integration, IDS should deal with the corresponding difficulties. IDS should address the accompanying issues, paying little mind to your decisions of supplies or network integration. It is necessary that it must run consistently without human supervision. It is a must that the system ought to be sufficiently dependable to permit it to run in background of the system being watched. Also, a system crash must be survived without obliging the reconstructing of the IDS's information base each one time the system gets restarted. Also, it must oppose subversion. The system ought to screen itself to guarantee that it has not been subverted? It must force negligible overhead on the attacked network and watch deviations from ordinary conduct. It must be effectively custom-made to the network being referred to. Each system has diverse utilization patterns, and the safeguard instruments ought to adjust effortlessly to these patterns. It must adapt to changing system conduct during that interval as new applications are generally added. The framework profile will change after some time, and the IDS must have the capacity to adjust and must be hard to trick; while it’s working, An IDS may mistakenly recognize an attack in one of these conceivable ways..

   - A false positive happens when a system characterizes an activity as anomalous (a possible intrusion) when it is appropriate; 2. A false negative happens when a real intrusive activity has happened however the system permits it to pass through as non-intrusive conduct; a subversion error can happen when an intruder alters the operation of the intrusion detector to constrain false negatives to happen. Users of the IDS will overlook its output if false positive errors will occur, as it will characterize authentic activities as intrusions. The events of this sort of error ought to be minimized in order

to give valuable data to the operators. In the event that an excess of false positives are created, the operators will come to overlook the output of the system over the long run, which may prompt an actual intrusion being detected however disregarded by the users. A false negative error happens when an activity returns despite the fact that it is an intrusion. False positive errors are less serious than false negative errors on the grounds that they give a deceptive feeling of security. By permitting all activities to continue, a suspicious activity won't be brought to the consideration of the operator. Since the security of the system is lessened from the state it was in before the intrusion detector was installed the IDS has currently a burden as stated in Junqi Wu (2008). Junqi Wu (2008) also claimed as an intruder could utilize information about the internals of IDS to modify its operation, perhaps permitting anomalous behavior to proceed further. The system's operational security imperatives could then damage by the intruder. A human detector can find this looking at the logs from the intrusion detector, however no doubt the IDS still is working accurately. From all these main issues related with IDS, it emphasizes on the need of such IDS that will have fast large and complex data processing and analysis of exact type of intrusion attack identification in the network with less human intervention and it must cover large extent of intrusion attack types. It gives an idea about integration of IDS detection techniques and use of more than single IDS in the network to cover known types of intrusions as well as unknown one. The issues and demerits related with single IDSs usages are described in chapter

- Additionally; it should response effectively to detected intrusion attacks to protect the vital resources of the organization before their damage or stealing. It is clearly stating that there should be integration of IDS along with IPS strategies to make the system more effective. Mainly, the effectiveness of IDS should be increased with detection rate of 100% along With least false positives as reported by Ciza Thomas (2009). The goal is still too far to achieve.

3. **Benefit of Integrating IPS Features with IDS:** Intrusion prevention systems are a sophisticated class of network security implementation that not only has the ability to detect the presence of intruder and their actions, but also has the ability to prevent them from such attacks. IPS incorporates the security features of firewall technology and that of IDSs. They can be viewed as a successful integration of both security technologies for higher and broader security measures. Because IPS combines all the levels of firewall and IDS technologies, they often end up with systems that function at altogether altitudes of the system stack.

V. PROBLEM ON HAND

It recognizes that as documented by F.Gong (2002), no one technique or invention is the silver bullet to provide protection against future attacks. Each of the three methods of intrusion discovery—signature detection, anomaly detection, and denial of service location and prevention—must be used to effectively defend business and government systems against the entire spectrum of threats and vulnerabilities. It is not enough for an IDS to only detect attacks; rather, it must enable precise detection to prevent attacks from reaching and damaging sensitive system assets and data. Many IDS are equivalent to a state-of-the-art

Maginot Line without a comprehensive set of identification techniques and the ability to execute them in order to precisely prevent attacks.

As a means of dealing with this, researchers have begun to examine the state-of-the-art IDSs and the problems that have arisen alongside them.

Problem No.1: First, what are the main downsides of utilizing IDSs that are based on only one technique? Can a system be built that acts as its own IDS and detects both known and unknown forms of attack while minimizing the rate at which false positives and negatives are generated?

Problem No.2: For the second issue, it is abundantly clear that there is no silver bullet technology that can fix this. So can we build and construct system that will incorporate Signature Detection, Anomaly Detection approaches with their merits to handle this issue?

Problem No.3: Is it possible to prevent computer and network resources from data loss and damages with the provision of prevention steps invoked automatically, once known or unknown attack is detected in single IDS instead of separate deployment of IPS to do protection?

Problem No.4: This is undoubtedly a tough work and to make this system successful, there is requirement of approaches to handle vast quantity of data for any form of attack detection automatically instead of manually. When it comes to IDS, the question becomes whether or not data mining (DM) techniques can be used to conduct this work of efficient knowledge finding on autopilot.

Problem No.5: How to propose a construction modeling better than the abuse based or the aberrance based interruption identification looking into the expansive information set furthermore the element nature of the system environment. ?

Problem No.6: What are the execution parameters accessible for the real appraisal of IDSs?

Problem No.7: What are the constraints that can be raised and can be improved in future while implementing IDS and IPS features in integrated fashion?

Problem No.8: Will sentiment analysis study help to deal with false positives and false negatives in the IDS alerts effectively?

1. How can an advanced intrusion detection system be built automatically and systematically utilizing?

2. How can we minimize the time spent on system reconfiguration by network administrators by including preventative measures in the detection system itself?

3. How to employ sentiment analysis to boost its performance?

4. To automatically and methodically create flexible and extendable sophisticated intrusion detection system utilizing Data Mining methods.

5. To provide in-built prevention policies in the detection system so that it will reduce network administrator's system re-configuration efforts.

6. To give base of sentiment analysis to enhance IDSs performance."

VI. CONCLUSION

IDS has been a great tool for the detection of attack under any network computing environment since 1980 when James P. Anderson first introduced concept of automated IDS. The security features of IDS since then are increasing over the years. New features are being added day by day in recent IDS/IPS systems. Moreover, hardware tools are also getting smart and these also enhanced the security features of IDS. However, these systems might later work as the attack surface for the intruders, so it must be designed carefully.

Most of the IDS works on behavior and pattern of the previously known attack. Zero day attack are always seems to be challenging because of the fact that the system has no defined pattern and behavior of such malicious attacks. However, the advancement in security algorithm especially for AI and ML based algorithms has paved the path to strengthen the capabilities of IDS/IPS systems. By adding AI/ML capabilities to the IDS/IPS, the system can be made more effective in all sorts of network computing.

VII. REFERENCES

[1] **A. Lazarevic, L. Ertoz, V. Kumar, A. Ozgur, and J. Srivastava (2003)**, "A Comparative Study of Anomaly Detection Schemes in Network Intrusion Detection", In Proc. Third SIAM Conference on Data Mining, pp.1-12.
[2] **Abhi R. Varma,Seema V. Arote, Chetna Bharti, and Kuldeep Singh(2012)**, "Accident Prevention Using Eye Blinking and Head Movement", IJCA Proceedings on Emerging Trends in Computer Science and Information Technology-2012
[3] **Altwaijry H. and Algarny S. (2012)**, "Bayesian based intrusion detection system", In Journal of King Saud University – Computer and Information Sciences, pp.1-4.
[4] **Ankit Phadia (2007)**, "Intrusion Alerts", Indian Edition.
[5] **B. Casewell and J. Beale (2004)**, "SNORT 2.1, Intrusion Detection", Second Edition, Syngress.
[6] **Bing Liu (2010)**, "Sentiment Analysis: A Multi-Faceted Problem", IEEE Intelligent Systems, pp.1-5.
[7] **Chebrolu, S (2005)**, "Feature deduction and ensemble design of intrusion detection systems", Computers & Security, 2005-06
[8] **Diego Zamboni (1999)**, "Intrusion Classification", Available on: www.cerias.purdue.edu/about/history/coast_resources/idcontent/classification
[9] **D.E.Denning (1987)**, "An Intrusion Detection Model", SRI International, IEEE, pp. 118-129.
[10] **Kaleton (2002)** Internet, "Combination of Misuse and Anomaly Detection", Version 1.0 on: dl.packetstormsecurity.net/papers/IDS/kaletonidspaper.pdf
[11] **Meng, Yuxin, Yang Xiang, and LamForKwok. (2014)**, "Applications of Machine Learning in Intrusion Detection", The State of the Art in Intrusion Prevention and Detection, 2014.

