# Classification of IDSs and challenges

Gulshan Kumar

*Department of computer applications, SBS State Technical Campus*
*Ferozepur (Punjab)- India-152004*
gulshanahuja@gmail.com

*Abstract*— **Nowadays, the Internet is the thing that we all want and like. In most of the cases, we are dependent on its abilities like the ability to publish and find the information, the ability to perform online shopping, and the ability to communicate with others through various types of softwares. Unfortunately, most of the popular softwares contain vulnerabilities and configuration errors. The basic cause of these vulnerabilities is the software flaws. These flaws fail to work with all possible conditions, especially unusual user input. Finding and patching of all software flaws is a major problem of the industry. The malicious users exploit vulnerabilities in software to mount a variety of intrusions. The intrusions affect the users in multiple ways. The protection from intrusions enforces the organizations to bear the additional costs. But, the cost involved in protection from the intrusions is often insignificant when equated with the actual cost of a successful intrusion. This factor forces the necessity to develop an accurate intrusion detection system (IDS). Many efforts have been made for the development of an effective IDS. But, still IDSs have to face many challenges in providing true security against a variety of intrusions.**

**In this paper, we explored various IDSs and categorized them based upon their architectural components. The IDSs have been critically analyzed for major challenges and issues in detecting intrusions effectively. The study in this paper will help the better understanding of different directions in which research has been done in the field of intrusion detection. The findings of this paper provide useful insights into literature and are beneficial for those who are interested in applications and development of IDSs and related fields.**

*Keywords*— **Data Breaches, Intrusions, Intrusion detection, Intrusion detection system, Network Security, Security Threats.**

## I. INTRODUCTION

Advancement of Internet technologies leads to resource sharing and effective com-munications. Nowadays, we have increased our dependency over the Internet appli- cations in our daily life like accessing information, online shopping, online banking and business transactions etc. However, most of popular software has flaws and mis-configurations, which leads to the new avenue for intruders to attack important Internet resources. Many efforts have been done to prevent the Internet resources from various types of attacks. These attacks are generally classified into four categories viz. Probe, DoS, U2R and R2L. But, 100% prevention from attacks is not possible. So, we need to detect the attacks for appropriate corrective measures and to minimize the damage from these severe attacks. For the purpose, many intrusion detection systems (IDSs) have proposed in the recent past. Since the first model of IDS in 1980's, many IDSs have been proposed to improve the detection results also. But still IDSs are in the infancy stage as it has to face many challenges to achieve 100% detection results.

Article overview: following this introduction, section 2 highlights the impor- tant IDSs proposed in literature. Their types and general architecture with the components have been explained. Section 3 highlights important challenges and issues of the common IDSs. Finally, the paper concludes the current scenario of IDSs.

## II. INTRUSION DETECTION SYSTEMS

The notion of intrusion detection was originally suggested by [2]. He proposed that audit trails contain vital information that can be used to detect the intrusions. The same concept was further extended by [12] at SRI International. He suggested a solution to secure the computer systems by proposing the first model for an IDS called Intrusion Detection Expert System (IDES). The proposed IDS model is independent of any intrusion, the system and its environment. The model is based on the concept that the intrusion is the abnormal usage of system resources. The model proved as an abstract model for further improvements. In 1988, Haystack IDS was developed at Lawrence Liver more Laboratories [38]. The concept of single IDS was further enhanced for Distributed Intrusion Detection System (DIDS) for client server architecture by releasing Stalker IDS [22]. Then, many commercial IDSs were introduced into the market. For example, Network Security Monitor (NSM), Net Ranger, Real Secure, Snort and many more [22, 19, 29]. Different IDSs possess different characteristics for meeting the requirements of an ideal IDS that involve the following [10]:

- Accurate: No False Positives.
- Complete: No False Negatives.
- Performance: Real Time Detection.
- Fault tolerance: The IDS not becoming security vulnerability itself.
- Scalability/Timeliness: Process large amounts of audit data quickly to prop- gate intrusion information for counter measures.

In spite of many efforts till date, IDSs have to face many challenges in meeting the requirements of an ideal IDS.

 

### A. Architecture

Many research efforts have been applied to make the IDS more effective and ac- curate. The focus was on developing a new system architectures and detection techniques to meet the requirements of an ideal IDS. With the passage of time and growth of computer attacks, several IDSs architectures have been proposed. [4] Proposed a common architecture for IDS as depicted in Fig. 1.

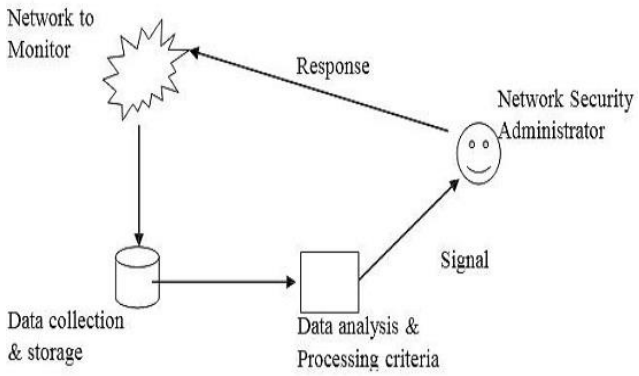


Fig. 1 Architecture of IDS

The components of common architecture are as described below:

- Network to monitor is the identity to be monitored for the intrusions. This can be a single host or a network.
- Data collection & storage unit is responsible for collecting the data of various events, converts it in a proper format and stores it to disk.
- Data analysis & processing unit is the brain of the IDS. It contains the whole functionality to find the suspicious behavior of attack traffic. On detect- ing the attack, a signal is generated. Based on the type of the IDS, action can be raised by the system itself to alleviate the problem or signal is passed to the network administrator to take the appropriate action.
- Signal part of the system handles all output from the IDS. The output may be either an automated response to an intrusion or alert of malicious activity for a network security administrator.

A large number of techniques have been developed to analyze data for detecting intrusive behavior of actions by Data analysis & processing unit. From late 1980s to early 1990s, the hybrid approach of expert systems and statistical techniques were utilized. Security expert knowledge was utilized to frame rules for the expert systems. Till late 1990s, the manual coding was shifted to automatic rule genera- tion that defines the normal or abnormal behavior. After that various techniques from a wide range of disciplines have been utilized in the later developments. Current research on developing accurate & efficient IDS presents new areas of research, which include artificial intelligence, data mining [26], statistical techniques [12], agent frameworks including autonomous agents [5], intelligent agents and mobile agents [3] for distributed intrusion detection. However, there is still room for an improvement in these techniques to make an IDS more accurate and efficient.

Article overview: following this introduction, section 2 highlights the important studies of mutual information (MI) based feature selection for intrusion detection. The section also presents the basic concepts and related work in the field. Finally, the paper concludes the current scenario of MI based feature selection techniques in general and especially for intrusion detection.

### B. Types

An intrusion detection system (IDS) defined as “an effective security technology, which can detect, prevent and possibly react to the computer attacks ”is one of the standard components in security infrastructures [17, 25]. It monitors target sources of activities, such as audit and network traffic data in a computer or net- work systems and deploys various techniques in order to provide security services. The main objective of an IDS is to detect all intrusions in an efficient & effective manner. Several types of IDSs have been developed that use different types of audit data, employ different types of techniques to analyze the data, and produce different types of output signals. Therefore, the IDSs can be categorized into vari- ous classes depending upon the type of data utilized, type of technique employed, and type of output signal produced by different modules of the IDS as depicted in Fig. 1. Based on data collection & storage unit, IDSs can be divided into two classes:

- Host based IDSs: Host based IDSs collect the data from the host to be protected. They collect the data generally from system calls, the operating system log files, NT events log file, CPU utilization, application log files, etc. Advantages of host based IDSs are that they are operating system dependent & are very efficient to detect attacks like buffer overflow. These systems become inefficient in the case of encrypted data and switched network. Major host based IDSs available are MIDAS [35], Haystack [38], Intrusion Detection Expert System (IDES) [28] , Tripwire [24], OSSEC HIDS [18], and Samhain [34].
- Network based IDSs: Network based IDSs collect the data from the network di- rectly in the form of packets. These IDSs are operating system independent and easy to deploy to various networks. Major network based IDSs available are NSM [19], NADIR-Network Anomaly Detector and Intrusion Reporter [20], EMERLARD [33], Bro [32], Snort [6], and Cisco Secure [36].

 

Based on criteria adopted for data analysis & processing unit, IDSs can be divided into two classes:

- Misuse or signature based IDSs: Signature based IDSs maintain a database of known attack signatures. The detection of attack involves comparison of data from the data collection unit and data stored in the database. If the match occurs then attack signal get generated. Signature based IDSs have very low false alarm rate. But, difficult and challenging task is to keep the database of signatures up to date. Signature based IDSs performs well for attacks whose signatures are in the database but they are inefficient to detect zero day attacks. Most of the commercially available IDSs belong to this category. Major signature based IDSs available are ASAX [17], USTAT [21], IDIOT [9], GrIDS [41], Tripwire [24], Bro [32], and Real Secure (Internet Security Systems [42]).
- Anomaly based IDSs: Anomaly based IDSs react to anomalous behavior as de- fined by some history of the monitoring systems, previous behavior or some previously defined profile of that system. The system matches the current pro- file with the previous profile. If there is any significant deviation, then that activity is notified as an attack. These systems are capable of detecting zero day attacks. Major anomaly based IDSs available are IDES [28], W & S [44], Comp Watch [13], AAFID-Autonomous Agents for Intrusion Detection [40], and NADIR-Network Anomaly Detector and Intrusion Reporter [20].

Depending on criteria adopted for generating the response, IDSs can be divided into two classes:

- Passive IDSs: Passive IDSs response to the attacks by generating signals for net- work administrator or the user to take appropriate action. They do not them- selves try to mitigate the damage done, or actively seek to harm or hamper the attacker. Major IDSs in this class are IDES [28], GrIDS [41], and NIDES [1].
- Active IDSs: Active IDSs response to attacks by initiating certain action automat- ically. The action can be against two entities, which further classifies active IDS into subclasses. These entities can be: Attacking system: In this class, IDSs try to control the attacking system. Here, IDSs try to attack the attacker's system to remove his platform of operation. Attacked system: In this class, IDSs try to control the attacked system. They modify the state of the victim system to mitigate the attack. They can terminate the network connections, increase the security logging or kill the concerned processes, etc. Major IDSs in this category are EMERLARD [33], Janus [16], OSSEC HIDS [18], and RealSecure (Internet Security Systems [42]).

The above discussion on types of IDSs can be summarized in Table 1.

TABLE I
SUMMARY OF VARIOUS TYPES OF IDSS

| IDS | Criteria | Audit Data | Response |
|---|---|---|---|
| NSM [19] | Hybrid | Network | Passive |
| Bro [32] | Signature | Network | Passive |
| MIDAS [35] | Hybrid | Host | Passive |
| Haystack [38] | Hybrid | Host | Passive |
| IDES [28] | Anomaly | Host | Passive |
| W & S [44] | Anomaly | Host | Passive |
| Comp Watch [13] | Anomaly | Host | Passive |
| ASAX [17] | Signature | Host | Passive |
| USTAT [21] | Signature | Host | Passive |
| IDIOT [9] | Signature | Host | Passive |
| GrIDS [41] | Hybrid | Hybrid | Passive |
| NIDES [1] | Hybrid | Host | Passive |
| EMERLARD [33] | Hybrid | Hybrid | Active |
| Janus [16] | Signature | Host | Active |
| Tripwire [24] | Signature | Host | Passive |
| OSSEC HIDS [18] | Hybrid | Host | Active |
| Snort [6] | Hybrid | Network | Active |
| AAFID [40] | Anomaly | Host | Active |
| NAIDR [20] | Anomaly | Network | Passive |
| Real Secure [42] | Signature | Hybrid | Active |

## III. CHALLENGES AND ISSUES OF THE IDSS

In the real world, ID process involves the processing of high dimensional net- work & audit data. Processing of high dimensional data is highly computationally expensive. It may lose the real time analysis capability of an IDS. So, there is a requirement to reduce the computational overhead to make an IDS fast and opera- tional in the real world. The computational overhead may be reduced by applying appropriate feature selection technique that selects relevant and non-redundant features. Another significant problem for the IDSs is the distribution of the data that is also dynamic changing with the passage of time. The data may have pat- terns of novel attacks. Non-availability of signatures of the novel attacks in the database of the IDS leads to high false alarm rate and low detection accuracy. In fact, practitioners as well as researchers have observed that an IDS can easily trig- ger thousands of alarms per day, up to 99% of which are false positives (i.e. alarms that were mistakenly triggered as malicious events) [23]. Most of the attacks are likely to generate multiple related alarms. This flood of false alarms makes it very difficult to identify the hidden true positives (i.e. those alarms that correctly flag attacks) [23]. The current IDSs do not make it easy for network administrators to logically group related alerts, and is

 

another problem with the current IDSs [11]. The most appealing way to reduce false alarms is to develop a better IDS that generate fewer false alarms. The process of reducing the false alarms is very chal- lenging because false alarms are the result of many problems. The major problems include the following:

- Low detection efficiency & high false alarm rate [8, 15, 45].
- Low throughput and the high cost, mainly due to higher data rates (Gbps) that characterize current wide band transmission technologies [15].
- Processing of a large volume of data with less information loss [27, 45] and processing a large volume of data results extra computational overhead which in turns loses of a real-time analysis capability of an IDS [7, 37].
- Most of the existing intrusion detection techniques strive to obtain a single solution that lacks classification trade-offs [14].
- Non availability of a globally acceptable standard/metric for evaluating an IDS [31, 15].
- Lack of a standard evaluation dataset that can simulate realistic network en- vironments [31].
- Highly imbalanced attack class distribution [45].
- Continuous adaptation of an IDS to a constantly changing environment [45].
- The inherent problem of writing correct patterns for an IDSs [30, 14];
- Current IDS do not properly aggregate and correlate the alarms that leads to flood of false alarms for the network administrator [11].
- Network normal behavior can be subjective, and anomalies may not be well defined. Since, the normal profile is subject to the current state of normality in the network, which may be compromised by very low intensity attacks [27,45].
- Intrusion detection software mechanisms themselves are not inherently survivable; It lacks to defend itself from attacks [31, 15, 4].

These causes enforce an IDS to be fast, flexible (instead of strict thresholds), adap- tive (instead of fixed rules), dynamic learning of new patterns and aggregate logi- cally correlated false alarms to identify the root of alarms. Thus, an efficient IDS should address all these issues including reduction of false positives, fast processing of large volume of network traffic and adapting to the changing environment for the novel attacks.

Another significant challenge is the appropriate comparison of the IDSs against one another. The scarcity of an appropriate public dataset severely impairs the evaluation of the IDSs, particularly effecting anomaly based detectors. This has been pointed out in numerous work [43]. Even, [39] has also argued that "the most significant challenge an evaluation faces is the lack of appropriate public datasets for assessing anomaly detection systems ".

[1]

[2]

[3]

## IV. CONCLUSIONS

The aim of this paper is to present a classification of IDSs, their types, challenges and issues. The paper introduced need and significance of IDSs. Various IDSs are explored to access their challenges to detect intrusion effectively. The challenges and issues of IDSs listed in this paper will helps the readers to explore their research in the field of intrusion detection.

.

## REFERENCES


1. Anderson, D., Frivold, T., Valdes, A.: Next-generation intrusion detection expert system (NIDES): A summary. SRI International, Computer Science Laboratory (1995)
2. Anderson, J.P.: Computer security threat monitoring and surveillance. Tech. Rep. 79F26400, James P. Anderson Co., Fort Washington (1980). URL http://csrc.nist.gov/publications/history/ande80.pdf.
3. Asaka, M., Taguchi, A., Goto, S.: The implementation of ida: An intrusion detection agent system. In: Proc. of the 11th Annual FIRST Conference on Computer Security Incident Handling and Response (FIRST99). Citeseer (1999)
4. Axelsson, S.: Intrusion detection systems: A survey and taxonomy. Tech. rep., Technical report (2000)
5. Balasubramaniyan, J., Garcia-Fernandez, J., Isacoff, D., Spafford, E., Zamboni, D.: An architecture for intrusion detection using autonomous agents. In: Proc. 14th Annual Com- puter Security Applications Conference, pp. 13–24. IEEE (1998)
6. Beale, J., Baker, A., Caswell, B., Poor, M.: Snort 2.1 Intrusion Detection. Syngress Media Inc (2004)
7. Cannady, J., Harrell, J.: A comparative analysis of current intrusion detection technologies. In: Proc. of the Fourth Technology for Information Security Conference, vol. 96 (1996).
8. Chandola, V., Banerjee, A., Kumar, V.: Anomaly detection: A survey. ACM Computing Surveys (CSUR) 41(3), 15 (2009).
9. Crosbie, M., Dole, B., Ellis, T., Krsul, I.: E. spa ord. idiot-users guide. Tech. rep., Technical. Report TR-96-050, Purdue University, COAST Laboratory (1996).
10. Debar, H., Dacier, M., Wespi, A.: Towards a taxonomy of intrusion-detection systems. Computer Networks 31(8), 805–822 (1999).
11. Debar, H., Wespi, A.: Aggregation and correlation of intrusion-detection alerts. In: Proc. of Recent Advances in Intrusion Detection, pp. 85–103. Springer (2001)
12. Denning, D.: An intrusion-detection model. IEEE Transactions on Software Engineering (2), 222–232 (1987).
13. Dowell C, R.P.: The computerwatch data reduction tool. In: Proc. of the 13th national computer security conference, Washington, DC (1990).
14. Engen, V.: Machine learning for network based intrusion detection: an investigation into discrepancies in findings with the kdd cup'99 data set and multi-objective evolution of neural network classifier ensembles from imbalanced data. Ph.D. thesis, Bournemouth University (2010)
15. Garcia-Teodoro, P., Diaz-Verdejo, J., Macia-Fernandez, G., Vazquez, E.: Anomaly-based network intrusion detection: Techniques, systems and challenges. computers & security 28(1-2), 18–28 (2009)
16. Goldberg, I., Wagner, D., Thomas, R., Brewer, E.: A secure environment for untrusted helper applications confining the wily hacker. In: Proc. of the 6th conference on USENIX Security Symposium, Focusing on Applications of Cryptography, vol. 6, pp. 1–1. USENIX Association (1996)
17. Habra, N., Charlier, B., Mounji, A., Mathieu, I.: Asax: Software architecture and rule- based language for universal audit trail analysis. Computer Security - ESORICS 92 pp. 435–450 (1992)
18. Hay, A., Cid, D., Bray, R.: OSSEC host-based intrusion detection guide. Syngress (2008)
19. Heberlein, L., Dias, G., Levitt, K., Mukherjee, B., Wood, J., Wolber, D.: A network security monitor. In: Proc. of IEEE Computer Society Symposium on Research in Security and Privacy, pp. 296–304. IEEE (1990)
20. Hochberg, J., Jackson, K., Stallings, C., McClary, J., DuBois, D., Ford, J.: Nadir: An automated system for detecting network intrusion and misuse. Computers & Security 12(3), 235–248 (1993)


 

21. Ilgun, K., Kemmerer, R., Porras, P.: State transition analysis: A rule-based intrusion detection approach. IEEE Transactions on Software Engineering 21(3), 181–199 (1995)
22. Innella, P., et al.: The evolution of intrusion detection systems. SecurityFocus, November 16 (2001)
23. Julisch, K.: Clustering intrusion detection alarms to support root cause analysis. ACM Transactions on Information and System Security (TISSEC) 6(4), 443–471 (2003)
24. Kim, G., Spafford, E.: Tripwire: a case study in integrity monitoring. In: Proc. of Internet besieged, pp. 175–210. ACM Press/Addison-Wesley Publishing Co. (1997)
25. Kumar, G., Kumar, K., Sachdeva, M.: The use of artificial intelligence based techniques for intrusion detection: a review. Artificial Intelligence Review 34(4), 369–387 (2010)
26. Lee, W., Stolfo, S., Mok, K.: Adaptive intrusion detection: A data mining approach. Ar- tificial Intelligence Review 14(6), 533–567 (2000)
27. Lim, S., Jones, A.: Network anomaly detection system: The state of art of network be- haviour analysis. In: Proc. of International Conference on Convergence and Hybrid Infor- mation Technology (ICHIT), pp. 459–465. IEEE (2008)
28. Lunt, T., Tamaru, A., Gilham, F., Jagannathan, R., Jalali, C., Neumann, P., Javitz, H., Valdes, A., Garvey, T.: A real time intrusion detection expert system (ides). Interim Progress Report, Project 6784 (1990)
29. McHugh, J.: Intrusion and intrusion detection. International Journal of Information Se- curity 1(1), 14–35 (2001)
30. Owens, S., Levary, R.: An adaptive expert system approach for intrusion detection. Inter- national Journal of Security and Networks 1(3), 206–217 (2006)
31. Patcha, A., Park, J.M.: An overview of anomaly detection techniques: Existing solutions and latest technological trends. Computer Networks 51(12), 3448 – 3470 (2007). DOI 10.1016/j.comnet.2007.02.001.
32. Paxson, V.: Bro: A system for detecting network intruders in real-time. Computer networks 31(23), 2435–2463 (1999).
33. Porras, P., Neumann, P.: Emerald: Event monitoring enabling response to anomalous live disturbances. In: Proc. of the 20th national information systems security conference, pp. 353–365 (1997)
34. Samhain: The samhain file integrity/intrusion detection system. Samhain labs (2010). URL http://la-samhna.de/samhain/.
35. Sebring, M., Shellhouse, E., Hanna, M., Whitehurst, R.: Expert systems in intrusion detec- tion: A case study. In: Proc. of the 11th National Computer Security Conference, vol. 32 (1988)
36.Secure, C.: Ids (2010). URL http://www.cisco.com/warp/public/cc/pd/sqsw/sqidsz/index.shtml.
37. Singh, S., Silakari, S.: A survey of cyber attack detection systems. International Journal of Computer Science and Network Security 9(5), 1–10 (2009)
38. Smaha, S.: Haystack: An intrusion detection system. In: Proc. of fourth Aerospace Com- puter Security Applications Conference, pp. 37–44. IEEE (1988)
39. Sommer, R., Paxson, V.: Outside the closed world: On using machine learning for network intrusion detection. In: Proc. of IEEE Symposium on Security and Privacy (SP), pp. 305–316. IEEE (2010)
40. Spafford, E., Zamboni, D.: Intrusion detection using autonomous agents. Computer net- works 34(4), 547–570 (2000)
41.Staniford-Chen, S., Cheung, S., Crawford, R., Dilger, M., Frank, J., Hoagland, J., Levitt, K., Wee, C., Yip, R., Zerkle, D.: Grids-a graph based intrusion detection system for large networks. In: Proc. of 19th National Information Systems Security Conference, vol. 1, pp. 361–370. Baltimore (1996)
42. Systems, I.S.: Real secure (2012). URL http://www.iss.net
43. Tavallaee, M., Stakhanova, N., Ghorbani, A.: Toward credible evaluation of anomaly-based intrusion-detection methods. IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews 40(5), 516–524 (2010)
44. Vaccaro, H., Liepins, G.: Detection of anomalous computer session activity. In: Proc. Of IEEE Symposium on Security and Privacy, pp. 280–289. IEEE (1989)
45. Wu, S., Banzhaf, W.: The use of computational intelligence in intrusion detection systems: A review. Applied Soft Computing 10(1), 1–35 (2010)

 