A Survey On Intrusion Detection System

Aastha Puri¹, Nidhi Sharma²
Research Scholar¹, Assistant Professor²
SDDIET Department of Computer Sc. Barwala Haryana, India

Abstract - Intrusion detection in the computer networks has been a major research area from the past few years. Many new techniques have been evolved and compared with the existing approaches. The basis of comparison of such computer vulnerabilities have been the accuracy of detection and the and the failure rate. In the present paper several machine learning and other suitable approaches proposed to solve the problem of intrusion have been reviewed and conclusion on the basis of the performance parameters is drawn. In future the approach must be modified and results must be compared with the existing approaches.

Keyword - Intrusion Detection System, Security

INTRODUCTION

Networking is the practice of linking multiple computing devices together in order to share resources. These resources can be printers, CDs, files, or even electronic communications such as e-mails and instant messages. These networks can be created using several different methods, such as cables, telephone lines, satellites, radio waves, and infrared beams. Both traditional and modern forms of computer networking aim to provide users with the ability to share data amongst multiple gadgets, whether they be in the same building or across the globe. Traditional computer networking relied on Ethernet and fiber optic cables to connect various devices on a network. More modern technology has emerged that allows for wireless connections between electronics. These technologies include Wi-Fi and Bluetooth compatible devices.

Without the ability to network, businesses, government agencies, and schools would be unable to operate as efficiently as they do today. The ability for an office or school to connect dozens of computers to a single printer is a seemingly simple, yet extremely useful capability. Perhaps even more valuable is the ability to access the same data files from various computers throughout a building. This is incredibly useful for companies that may have files that require access by multiple employees daily. By utilizing networking, those same files could be made available to several employees on separate computers simultaneously, improving efficiency.

As the internet evolves and computer networks become bigger and bigger, network security has become one of the most important factors for companies to consider. Big enterprises like Microsoft are designing and building software products that need to be protected against foreign attacks. Anything from software, music and movies to books, games, etc. are stolen and copied because security is breached by malicious individuals. Today, most malicious users do not possess a high level of programming skills and instead make use of tools available on the Internet. There are several stages that an attacker has to pass through to successfully carry out an attack.

Network security refers to any activities designed to protect your network. Specifically, these activities protect the usability, reliability, integrity, and safety of your network and data. Effective network security targets a variety of threats and stops them from entering or spreading on your network. Network security is accomplished through hardware and software. The software must be constantly updated and managed to protect you from emerging threats. A network security system usually consists of many components. Ideally, all components work together, which minimizes maintenance and improves security.

IDS are one of many complementary layers of IT security technology. Several security layers exist because no one layer can provide all the security measures itself. IDS do several things that basic firewalls, for instance, cannot do: Identify anomalous packet content or patterns of traffic that are different from normal for any particular company’s network. Identify patterns, called signatures, of malicious content within packets coming into or leaving a company’s network.

The business benefit IDS provides is reducing the chance of missing security threats which could compromise confidentiality, integrity, privacy, or availability of mission critical assets and processes. An important consideration in lifecycle cost is managing and tuning out false positives generated by IDS. These activities are onerous and in my experience most network managers would rather outsource these tasks to experts. The next issue becomes selection of the appropriate IDS technology, which basically come in two flavours: network intrusion detection (NIDS or IDS) and host intrusion detection (HIDS). Network IDS sits on the network telecommunications media such as an Ethernet network or a wireless network, and passively monitors the contents of packets of information flowing in all directions. Host IDS is an entirely different ballgame. It has agents which reside on servers. It monitors several types of changes over time on servers which may indicate security problems.

Internet is a global public network. With the growth of the internet and its potential, there has been subsequent change in the business model of the organizations across the world. More and more people are getting connected to the internet every day to take advantage of the new business model popularly known as e-business. Internetwork connectivity has therefore become very critical aspect of today’s e-business. While an organization makes its information system available to harmless internet users, at the same time the information is available to the malicious users as well. Malicious users or hackers can get access to an
Intrusion Detection System (IDS) is always open to give a better result by applying such techniques to it which are feasible to merge with IDS. Applying meta-heuristic techniques to IDS has been a significant area of research for the researchers to come up with better algorithms to classify the intrusion on any system before blocking them. To achieve such real-time, accurate, and intelligent IDS, researchers are considering the ups and downs of various techniques. Also, the proper blend of the useful techniques can result in an ideal or near to ideal intrusion detection system.

Intrusion detection systems are those which check significant operation systems only. Host IDS is an entirely different ballgame. It has agents which reside on servers. It monitors several types of changes over time on servers which may indicate security problems. Host-based IDS system verifies malicious attacks at any kernel level or on operating system. This hybrid-based IDS are managing and alerting from both network and host-based intrusion detection devices and provide the logical complement to NID and HD - central intrusion detection management. The competence of IDS can be enhanced by making it capable of handling the large datasets. Hitherto, the techniques to carry out intrusion detection are boundless but they all lag behind in one feature or the other. Intrusion detection system is on which a large number of techniques can be combined and compared. For example, one can combine meta-heuristic based clustering with efficient feature selection technique. Hence, there is a tremendous future scope in the field of intrusion detection system, as one can consider the ups and downs of various techniques. Also, the proper blend of the useful techniques can result in an ideal or near to ideal intrusion detection system.

Intrusion detection systems have become a wide research area for the researchers to come up with a better algorithm to classify the intrusion on any system before blocking them. To achieve such real-time, accurate, and intelligent IDS, researchers are applying meta-heuristic techniques to IDS. Since there is a wide research going on in the field of meta-heuristic technique and IDS is always open to give a better result by applying such technique to it which are feasible to merge with IDS.

CONCLUSION

Many approaches have been used in the security analysis of computer networks. In one approach, Particle Swarm Optimization algorithm is used with the unsupervised classification algorithm. The IDCPSO technique shows higher speed of convergence and high detection rate as compared to the genetic approach. In another method, PSO algorithm is used with the Map Reduce approach which improves the parallelization in the approach of data mining. The detection in large amount of data is improved and the speed of operation is improved as compared to the basic approach. Some use unsupervised clustering using the grid based and density-based approaches. This helps improving the anomaly detection rate of the process. In future, several other machine algorithms must be implemented with unsupervised clustering approaches.

REFERENCES:


