Intrusion Detection System – A Literature Review

APL Madushanka, RPS Kathriarachchi, WAAM Wanniarachchi

Department of Information Technology, Faculty of Computing, General Sir John Kotelawala Defence University, Ratmalana, Sri Lanka

Abstract. With the advancement in technology, the day-to-day life of people is mostly dependent on technology. So, it is highly required to assure the reliability of network operations. There is a dramatic increase in the number of network attacks during recent years. With this, research interest in Intrusion Detection and Intrusion Detection System (IDS) have increased consequently. Intrusions into computer Systems by unauthorized users have become a rapidly growing problem with the increase in reliance on the internet, intranet, and extranet in network computer access. Unauthorized access to computer Systems or unauthorized activity in a computer or information system is defined as an intrusion. When considering the security of the computer system, intrusion detection technologies play an extremely important role. IDS can protect both internal and external parties. Although there were different intrusion detection systems have been implemented, none of the systems are capable of being completely flawless. This paper reviews new trends in intrusion detection and current intrusion detection systems. The main objective of this research is to presents a complete study about intrusion detection, failure points, advantages and disadvantages, special features, techniques, methods used, algorithms used, technologies, and concepts used in current intrusion detection systems. When considering the surveyed literature, it is clear that there is a requirement of securing the network against novel attacks. In some instances, the solution can be given as a hybrid, which means the combination of anomaly-based- intrusion detection and signature-based intrusion in providing the most effective solution for some attacks. And finally, implementing an intrusion detection system for research purposes is the ultimate goal. That system is having the capability of detecting and preventing intrusions and intruders.

Keywords: *Intrusion Detection System, Intrusion Detection, IDS Techniques, IDS and Machine Learning, IDS and Data Mining, Hybrid IDS*