Classification Model for Intrusion Detection

A. Ganesan[1], A. Kumar Kompaiya[2]
Department of Computer Applications
[1]PG & Research,Hindusthan Arts College, Coimbatore – 641 028, India.
[2]Chikkanna Govt. Arts College, Thiruppur – 641 602, India

Abstract-*This paper describes the possible factors of security violation and how the security breaks are classified. With the growth of internet or networked computer and associated applications, the Intrusion Detection system and its model are essential to keep resources (Hardware/Software) secure. An Intrusion Detection is a type of Security management system which gathers and analyzes the information from various areas with a computer or a network to identify possible security breaks which includes attacks from outside the organization (intrusion) and attacks from within the organization (misuses).*

Keywords-Intrusion Detection, Network, Internet, Malicious.

I. INTRODUCTION

The computer networks are used to transmit the data from one location to another location. The Internet is used to transmit data all over the world. With the growth of these communication technologies, a lot of online applications are designed such as online banking and online purchasing. While implementing this kind of network or internet based applications data can be transmitted through the different computer system (Routers or gateway / workstation). Due to the data transmission from outside environment data can be accessed by attackers or hackers to misuse or destroy the available data.

In general, a flow of data occurs from the source computer to a destination computer over a communication channel (wire / data bus).The security system is needed to restrict access to this data or information or file. Only the sender and receiver should have the access rights according to the security policy. Therefore to increase confidentiality of the network security and availability of data or information stored on the computer system, we need to have automated tools for protecting data or files stored on the computer and also to give alert to the administrator. This system is known as Intrusion Detection System. This paper describes the possible problems faced when we transmit the data through the network or internet and how the problem's solutions are classified.

II. INTRUSION DETECTION SYSTEM

Intrusion is defined as a malicious activity that is someone or something to compromise information system through malicious activity or security policy violation. An Intrusion Detection System is a device or software application that monitors a network or system for malicious activity or security policy violation. Any detected activity is reported to an administrator or security event management system. To identify possible security breaches which include both intrusion and misuse within the system or network, an intrusion detection system gathers and analyzes information from various areas. This intrusion detection system automatically alerts the administrator when someone tries to compromise the information system.

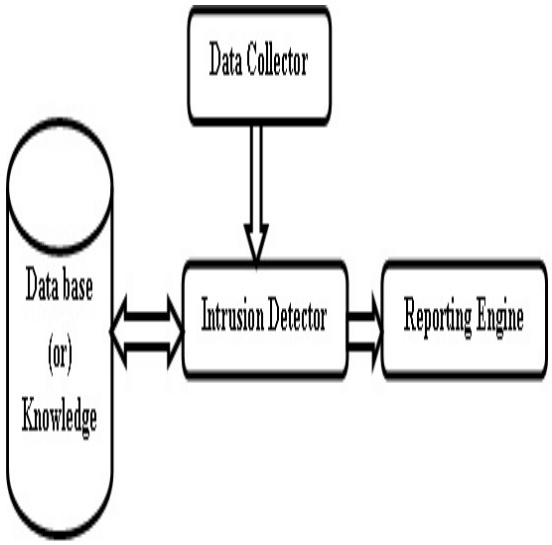

Figure 1: Intrusion detection system

III. CLASSIFICATION MODEL

The intrusion detection is classified into two broad categories, ie, host base intrusion detection and network based intrusion detection. In host base intrusion detection system (IDS), the IDS monitor host system activities such as operating system, system logs, application programs, files and so on. In network based IDS model, IDS placed on the network, it should examine network traffic, network pockets. The both network and host based IDS further classified into three categories. They are statistical model; Artificial intelligent based expert's system model and data mining model.

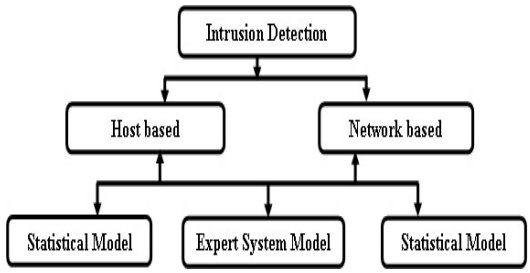

Figure 2: Classification model of intrusion detection system

3.1 Statistical Model

The purpose of statistical model to determine whether a new observations of user behavior is abnormal with respect to the previously collected user behavioral observations (Data base / Knowledge base). This model includes operational model, Mean medians standard deviation and coefficient of variants and multivariants models.

In statistical models the user profiles are used for measuring login and session action, file access and program usage. The profile used to measure user activity, login action, location details, last login, session elapsed time, password failure, output of session and program execution.

3.2. Expert System Based Model

Intrusion can be detected by using another one method artificial intelligence based expert system model. This system act as human expertise. The components of experts system include knowledge base which contains possible user traffic as logic representations. Information engine is another component. It is used to derive the knowledge from knowledge base whenever the explanation is needed. The knowledge base wise provide explanation. The Third component of expert system include user interface. It is used to access the knowledge base and to provide the query to the system. In knowledge base we can specify the user profile, time and date of access, user location, user id and type of access. The current time, location could be composed to the user profile to determine if the user is original user of the user id verified in the profile.

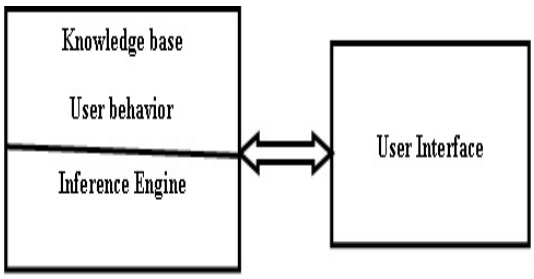

Figure 3: Expert system based model

The expert system are called as knowledge based intrusion detection system knowledge based accumulates. The knowledge about specific attack and vulnerabilities the system.

3.3. Data Mining Model

The data mining model, we can use association rule method, classification method, clustering, genetic algorithm, artificial neural network, query tools and decision tree method to detect intrusion. The classification method will reduce a number of records to be tested for intrusion. Association rule used to map the user behavior parameter (ex: password, file and location). Which is used to test abnormal behaviors of occurred in the network or host. The data mining method is used to detect the intrusion. This method deployed when huge amount of repertory involved indentifying intrusion to end to provide the response was quickly. The data mining method can further classify with clustering, classification. Association rule, genetic algorithm, artificial neural network, fuzzy logic.

IV. CONCLUSION

The classification model for intrusion detection system classifying the basic methods of intrusion detection system. This paper exhibits good performance in detecting categories of intrusion Detection, ie, network based IDS and host based IDS as well as how the methods are classified to detect intrusion in both categories. Using this model, we can identify where and when which type of efficient model is need for detect intrusion. ie, where and when statistical model, expert's system model and data mining model is need for intrusion detection. We can deploy effective, efficient and faster method to detect intrusion.

REFERENCES

[1] Andersion, J. (1995) An Introduction to neural networks, Cambridge: MIT Press.
[2] Canady J. (1998). Artificial neural networks for Misuse detection, Proceedings of the 1998 Nation information systems security Conference (NISSC'98), pp- 443-456, Arlington, VA.
[3] R. Agrawal, T Imielinski, and A. Ss. 1993. Mining Association Rules between Sets of Items in Large Databases. In Proceedings of the ACM SIGMOD Int'l Conf. on the Management of Data, pp. 207-216.
[4] K. Scarfone, P. Mell, Special Publication 800-94: Guide to Intrusion Detection and Prevention Systems (IDPS), National Institute of Standards and Technology (NIST) (2007).

[5] T. Abbes, A. Bouhoula, and M. Rusinowitch, Protocol analysis in intrusion detection using decision tree, Proceedings of International Conference on Information Technology: Coding and Computing (ITCC), vol. 1, 2004.
[6] A.A.E. Ahmed and I. Traore, Detecting computer intrusions using behavioral biometrics, Third Annual Conference on Privacy, Security and Trust (PST), 2005.
[7] Balajinath and SV Raghavan, Intrusion detection through learning behavior model, Computer Communications 24 (2001), no. 12, 1202–1212.
[8] S. Antonatos, K.G. Anagnostakis, and E.P. Markatos, Generating realistic workloads for network intrusion detection systems, ACM SIGSOFT Software Engineering Notes 29 (2004),No. 1, 207–215.
[9] O. Depren, M. Topallar, E. Anarim, and M.K. Ciliz, An intelligent intrusion detection system (IDS) for anomaly and misuse detection in computer networks, Expert systems with Applications 29 (2005), no. 4, 713–722.
[10] AK Ghosh, J. Wanken, and F. Charron, Detecting anomalous and unknown intrusions against programs, Proceedings of the 14th Annual Computer Security Applications Conference (ACSAC' 98), 1998, pp. 259–267.
[11] Ko, D. A. Frincke, T. Goan, L. T. Heberlein, K. Levitt, B. Mukherjee, C. Wee, "Analysis of an Algorithm for Distributed Recognition and Accountability", 1st ACM Conference on Computer and Communication Security, pp. 154-164, 1993.
[12] L. Gasser, "An overview of DAI", Kluwer Academic Publisher, Boston 1992.
[13] M. Crosbie, E. H. Spafford, "Applying Genetic Programming to Intrusion Detection", Technical report, Computer Sciences Department, Purdue.
[14] Balasubramaniyan, J. O. Garcia-Fernadez, D. Isacoff, E. H. Spafford, D. Zamboni, "An Architecture for Intrusion Detection using Autonomous Agents", Technical report Coast-TR-98-05, Computer Sciences Department, Purdue University.
[15] E. Denning, "An Intrusion-Detection Models", IEEE Transactions on Software Engineering, Volume SE-13, No. 2, February 1987.